MENLO SECURITY

Palo Alto Prisma Access: Cloud Managed Integration Guide

May 2025

Table of Contents

1. Revision History	1
2. Use Cases for Integration with Palo Alto Prisma Access	2
2.1. Simplify User Policy Enforcement	2
2.2. Protecting High-Risk Users and Applications	2
2.3. Integration Benefits	3
2.4. Before You Begin	3
3. Palo Alto Networks Configuration	4
3.1. Block action integration method	4
3.2. Override action Integration method	7
3.3. Transparent redirection with Prisma Access Traffic Steering 1	3
3.4. Common Steps for any of the selected integration methods 2	23
4. Menlo Security Configuration	26
5. Troubleshooting	
5.1. Technical Support	27

1. Revision History

Release	Date	Change
May 2025	May 2025	Refined some screenshots
March 2025 (2.90.0.20)	10100 1010	Changed the "rekey_time" for IKE from (8 hours) to 3 hours in the Edit Menlo_Security_IKE screenshot and the "rekey_time" for Children from (1 hour) to 1.5 hours in the Edit Menlo_Security_IPSec screenshot.
November 2024 (2.90.0.16)	November 2024	Added a note to recommend enabling tunnel monitoring when configuring an IPsec tunnel.
2.86	October 2022	Initial release

2. Use Cases for Integration with Palo Alto Prisma Access

2.1. Simplify User Policy Enforcement

Challenge

The internet contains more than four billion websites, with millions more launched every month. Many are new and, therefore, uncategorized, while others are inaccessible because of "false positive" classification. This leaves organizations with the difficult choice to either allow or deny user access. Allowing access supports user productivity but increases cyber risk, whereas denying access limits productivity and dramatically increases help desk tickets requesting website categorizations and recategorizations.

Solution

Together, Prisma Access and the Menlo Secure Cloud Browser allow organizations to leverage the URL policy capabilities of Prisma Access and selectively steer specific websites – such as uncategorized websites or those that register a false positive – to the Menlo Secure Cloud Browser. This allows users to access such websites safely without risking the organization's security posture. Users will experience 100% native web browsing, and their web browsers will receive 100% safe visual components for local rendering.

2.2. Protecting High-Risk Users and Applications

Challenge

Many organizations have a group of users that may require elevated security while accessing websites. These users may be privileged administrators, or they may have access to highly secure systems (e.g. payment systems, SWIFT interbank transfer systems) from their devices. The extra level of security may also be mandated by industry or government regulations.

Solution

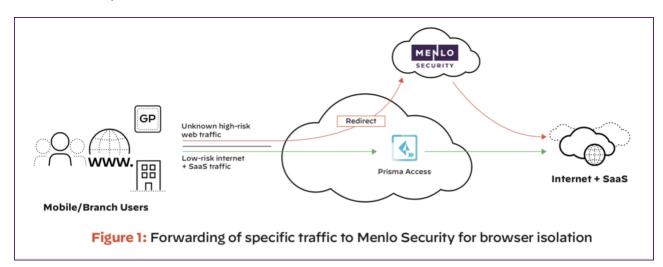
All web traffic for specific users or groups of users may be directed through the Menlo Secure Cloud Browser via integration with Prisma Access. This ensures any website the specified user or group accesses is executed within the Menlo Secure Cloud Browser, returning only safe and malware-free visual components to the user's device for local rendering in a web browser.

Prisma Access can integrate with Menlo Security to provide web isolation for users in two ways. The first method is via URL prepend, wherein URLs associated with a user's web traffic are prepended with safe[.]menlosecurity[.]com. The second method utilizes traffic steering policies in Prisma Access, wherein web traffic is redirected across an IPsec tunnel to the Menlo Secure Cloud Browser and is completely transparent to end users for a more seamless experience. End users will see no change and can browse web pages with a native experience.

2.3. Integration Benefits

Palo Alto Prisma Access and the Menlo Secure Cloud Browser work together to deliver the most proactive prevention posture available, while allowing enterprise users to be productive on the web and in email. The integrated solution:

- Stops malware from unknown/uncategorized websites.
- · Ends malware from weaponized documents and files.
- · Complies with regulations for air-gapping high-value users.
- Improves user productivity, unhindered by excessive website blocks.
- · Combines the benefits of Palo Alto Prisma Access policy and Isolation.
- · Reduces help desk tickets from users whose access to websites has been blocked.



2.4. Before You Begin

To ensure a smooth configuration process, please ensure the following prerequisites are met:

- Access to the Prisma Access instance and the Cloud Management portal managing it (similar steps as below could be followed in case the Prisma Access is managed via the Cloud Management platform).
- · Access to a Menlo Security instance and the Admin Portal (admin.menlosecurity.com).

3. Palo Alto Networks Configuration

The redirection of the specific traffic that is traversing Prisma Access towards the Menlo Secure Cloud Browser can be achieved in two ways:

- 1. Using categorization to redirect web requests to prepend isolation mode. This can be done two ways:
 - a. By a **block** action set to the desired URL Category and a custom Block Response Page.
 - b. By an **override** action set to the desired URL Category, that can then be applied to a security policy for a specific set of users; this integration method is not supported for the Explicit Proxy Mobile Users.
- 2. Transparent forwarding using Traffic Steering policies in Prisma Access and IPSec tunnels between the two cloud security solutions.

3.1. Block action integration method

Step 1: Set the desired URL Filtering Category to Block

Log into the Prisma Access Cloud Management portal and navigate to *Manage* > *Configuration* > *URL Access Management* > select **Mobile Users** context > *Access Control* tab > under **URL Access Management Profiles**, click **Add Profile**.

4	Manage		► URLAO								Puh Conf	8~
	Service Setup +	Control	RL Access Management (Mobile Users -) trai users' access to web context, and how they interact with it (Bir example, to prevent phishing, block users from submitting order predentation to non-composite sited. Also enforce and search engines like Coople and Bing.									
0	Configuration			io no Settir			or search engines like G	oogle and Bing.				
•	Security Policy Arti-Spyware	G	AdeNewl	itter							ResetFilt	ters
	Weinerability Protection WildFire and Antivirus DNS Security	The	profiles here a	re ac	igement Profil the only when you a security rule.	les (3) add them to a profile group	p. and Q. Searc	h 🖸	Delete	Care Ma	ANTO	
-	URL Access Management									5147		
	File Blocking HTTP Header Insertion		Name		BPA Verdict	Location	Security _	Profile Gr	Allow	Aiert.	Cont	
	Profile Groups		best-grac	â	O Pana	predefined	6/14	best-practice	7	52		2
	SaaS Application Management		Explicit P.,	4	O Pass	predefined	0/14	Explicit Provy	80			
	Decryption		Menip-U.		O Fal	Prisma Access	\$7.94	Mento-sec	74			
*	Network Services 🛩											
?	Identity Services +	504	the at your seco	rites	policy rules are usit	ng a URL Access Manageme	ent profile (7 at 54 rules	1				
	Objects 👻											
-			stom URL (-							
ø			ryide URL cate spories,	gory	erforcement with	your own custom URL	Q. Search			Nelete Chave	Add Catego	a
=									Used In			

Add a new URL Access Management Profile or edit an existing one (a similar Profile can be defined for the Remote Networks).

For the URL Categories that need to be redirected to Menlo Security for Web Isolation, set the Site Access to **Block**; the same access can be set for Custom URL Categories if needed.

4	Manage		Add URL Access Management Profile > URL Access Management Profile - Mobile Users 22 Best Practice Checks 22 Best Practice Checks										
	Service Setup +	_	-		partner in Pr	onne							
0	Configuration Security Services Security Policy	+ Nam		Unge			Categories to block for redirection to isolation						
8	Anti-Spyware Weinerability Protection												
	WidFire and Anthrop												
-	DNS Security URL Access Management File Blocking HTTP Header Intertion Profile Crosen		Coess Contro FOI classifier webs	s il Item hasked on site co	terit, Seatures, an Est Access -	6 salety: fait Scherkales -	User Credential Detection Detect when users attempt to submit corporate credentials to a website. User Credential Detection Disabled v						
	Sad Application Management Decryption		Category	Site Access	User Gred	His	Advantad UPI Julius Colonadaulius						
	Network Services v	-	dimain	Internet of	1 1000		Advanced URL Inline Categorization						
	identity Services +	-	news	Buck v	- stime		Enable cloud Inline Categorization						
•	Objects v			Alert			Enable local inline Categorization						
?			nudity	Allow	* afters		Exclude custom URI, categories or external dynamic lists from Inline Machine						
			online storage	Buck	• allow	1.2	Learning actions.						
		+ Regi	and Field	Continue			Canar .						

Step 2: Upload a custom Block Response Page

The custom Block Response Page has the role of prepending safe.menlosecurity.com in front of the original URL requested by the user, once that URL matches the URL Category we want to send through isolation.

Under URL Access Management > Settings, upload the custom Block Response page under the URL Access Management Block Page.

4	Manage		 URL Access Management Settings 			Push Carify -
	Service Setup	· Control	Access Management (theriach with it (har example, ha prevent		
6	Configuration Security Services	-	de credentials to non-corporate sites). Also en Control (Settings) Best Practices	force cale wards for wards engines i	ike Geogle and Bing.	_
	Security Policy	10	Location	551/TLS Service Profile	Mode	Properties
3	Anti-Spyware Vulnerability Protection	0	Prisma Access		redirect	address safe-merikanisarity.com
L.	WidFire and Antivirus					
	DNI Security					
	Uill Access Management File Blocking HTTP Header Insertion Profile Groups Saci Application Managem Description	Res	sponse Pages (5) Agent the web pages that are displayed when	ortan action are biggered.		
	File Blocking HTTP Header Insertion Profile Groups Sadi Application Manager Decryption Network Services	- Res		tertan action are Viggend.	Actions	
	File Blocking HTTP Header Insertion Profile Groups Seati Application Managem Decryption	- Carl	figure the web pages that are displayed when			
	File Blocking HETP Header Insection Profile Groups Said Application Manager Desryption Network Services Membry Services	- Carl - Peop - And I	Apers the web papes that are displayed where once Pape	location	Export®	
	File Blocking HETP Header Insection Profile Groups Said Application Manager Desryption Network Services Membry Services	Res Carl Prop Activ	Apers the web pages that are displayed when once Page Problem Block Page	Location prodefined	Export P	(TML Template
	File Blocking HETP Header Insection Profile Groups Said Application Manager Desryption Network Services Membry Services	- Res - Resp - Resp - Accil Accil	Agers the own pages that are displayed when once Page Product Block Page Philolog Continue Page	Location problemed problemed	Export P Export P Export P Reverts	(TML Template (TML Template

An example of a Block Response page is provided below and can be changed and adapted for more specific use-cases.

Custom Block Response page example:

```
<html>
<head>
<title>Web Page Blocked</title>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8">
<META HTTP-EQUIV="PRAGMA" CONTENT="NO-CACHE">
<meta name="viewport" content="initial-scale=1.0">
<style>
  #content {
    border:3px solid#aaa;
    background-color:#fff;
    margin:1.5em;
    padding:1.5em;
    font-family:Tahoma,Helvetica,Arial,sans-serif;
    font-size:lem;
  }
 h1 {
    font-size:1.3em;
    font-weight:bold;
    color:#196390;
  }
 b {
    font-weight:normal;
```

```
color:#196390;
  }
</style>
<script>
 var dest = "<url/>";
 var category = "<category/>";
 switch (category) {
    case 'questionable':
    case 'dynamic-dns':
    case 'unknown':
    case 'parked':
       var prepended = "https://safe.menlosecurity.com/";
       window.location.replace(prepended);
  }
// window.location.replace('https://safe.menlosecurity.com')
</script>
</head>
<body bgcolor="#e7e8e9">
<div id="content">
<h1>Web Page Blocked</h1>
Access to the web page you were trying to visit has been
blocked in
accordance with company policy. Please contact your system
administrator
if you believe this is in error.
<b>User:</b> <user/> 
<b>URL:</b> <url/> 
<b>Category:</b> <category/> 
To view the page in <b>Isolation</b>
</div>
</body>
</html>
```

Please continue with Step 3 as the configuration is similar for both methods from that point on.

3.2. Override action Integration method

Step 1: Set the desired URL Filtering Category to Override

Log into the Prisma Access Cloud Management portal and navigate to Manage > Configuration > URL Access Management.

Under the *Mobile Users* context, add a new **URL Access Management Profile** or edit an existing one (a similar Profile can be defined for the Remote Networks).

4	Manage				> URLAccess	lanagement Profile - I	Mobile Uvers
	Service Setup +		nlo-Securi				Sill and Langer fragment
0	Configuration +	* Nam		voge			Orweighter
۰	Security Services +	Meril	io-Security				Categories to override for redirection to isolation
8	Anti-Spyware Vulnerability Protection		y Rules Using This Groups Containing				
	WidFire and Anthreas						
•	DNS.Security URLAccess.Management FileBlocking		cess Contro	l Res based on site cor	tont, features, and	f safety.	User Credential Detection Detect when users attempt to submit corporate credentials to a website.
	HTTP Header Insertion Profile Groups		Q, Search		SetAcom -	Set Submission -	User Credential Detection Disabled +
	Sad Application Management		Category	Site Access	User Cred	1620	
	Decryption Network Services +		registered- domain				Advanced URL Inline Categorization
	Identity Services +	0	news	jOverside v	• silou	-	Enable cloud Inline Categorization
	Objects *		not-resolved	Net	+ allow	24	Enable local Inline Categorization
?			nudity	Allow	+ allow		Exclude custom URL sategories or external dynamic lists from index Machine
			ardine storage-	Buck	* alize	-	Learning actions.
		+ Rep	ind Field	Continue			Canal See
			and and a	Override			

For the URL Categories that need to be redirected to Menlo Security for Web Isolation, set the Site Access to override; the same access can be set for Custom URL Categories if needed.

Click **Save** to accept changes.

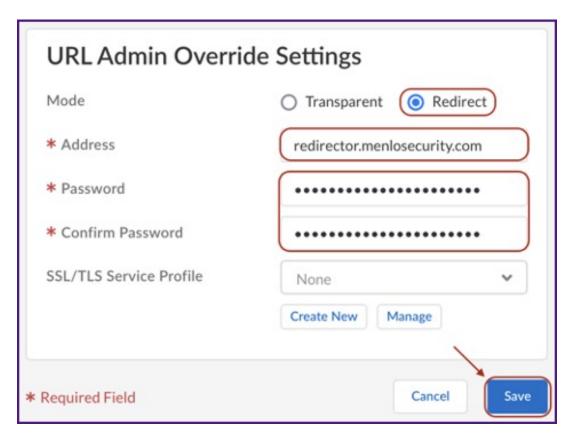
Step 2: Set the destination address to be used for the Override action

Under the same URL Access management tab, navigate to *Settings > URL Admin Overrides* and click **Add URL Admin Overrides**. In the *URL Admin Override* pane, click **Add**.

4	Manage	Manage > URLAccessManagement 3			Puch Config +
			low they interact with 8, flur example, to preven		
0	Configuration + Security Services +	Access Cantrol Settings Best Pr	n), Also inforce safe search for search engines actions	the Google and Bing.	
8	Security Policy Anti-Spymare	General Settings - Detault	0-	Remote Browser Isolation Sett	Sing - behavited from Shared
•	Vulnerability Protection WildFire and Anth-Inco DNL Security	URI, Continue Timeout (min) URI, Admin Override Timeout (min)	15 minutes 15 minutes	Remote Browser Isolation	Disabled
	UBL Access Hangement File Blocking HITTP Header Insertion Proble Groups Sadi Application Hangement	URL Admin Lockout Teremut (nord) Hold Client Report for Category Lookop Category Lookop Timeout Append End Token to List Entrins INNI OB Server	30 minutes M 2 miconels M Default		
	Decryption Network Services v	URLAdmin Overrides [0]			Tables Real Life, Administ Description
**	Objects +	a location	SSI/TLS Service Profile	Mode	Properties
?				0	
				es bicket UR, categories.	

In the URL Admin Override pane, fill in the form fields with the following values:

- Mode: Redirect
- · Address: redirector.menlosecurity.com
- **Password** and **Confirm Password**: Any password: this is the password that you share with your users who are allowed the override privilege. This is not used in the Menlo Security integration.
- SSL/TLS Service Profile: None



Continue with Step 3 as the configuration is similar for both methods from that point on.

Step 3: Update the policy handling the Internet bound traffic with the previously created URL Access Management profile

Navigate to *Configuration > Profile Groups >* select the *Mobile Users* context > click **Add Profile Group**

Add or edit an existing Profile Group using the previously configured URL Access Management Profile.

Manage				ellers	2						Push Config ~
	Security profiles -	car traffic	for threats, and	a profile group is	a solvection of each 1		-				
Configuration •					g po transerej ane i	eraci die prosp	Q s	sarch			
Security Services A Security Policy Acti-Seyware Valuerability Protection Wilfire and Activitys DNS-Security UELAccess Management File Blocking HETTP Header Insertion Prote Groups Sault Application Management Decryption –	Same	×- 8	Location productional productional	Ardi Profile best pra	Weinrablit Profile best-practice best-practice	URL Profile best prik. Explicit	File_ Profile least-pra_	El HIT_ Puble	Down Own Widffre Profile best-practice best-practice	DAG Profile best pr	Days Un
Manage				sup - Mobile User	5						
Configuration +	Configuration										
Security Services • Security Policy Anti-Speware Valenziality Protection WildFire and Activity DRS Security URS Access Management File Blocking HTTP Header Insertion	 Name Anti-Spyword Vulnerability URL Access N Profile 	Profile Protection Garagemen	Public in	tone Ione Merila-Security	die				* * * *		
	Service Setup Configuration Security Services Security Policy Acti-Service Setup Utherability Protection Welffire and Activity Uth Access Management Fill Distance Insertion Public Groups Inst Apple atom Management Description Teach Apple atom Management Description Teach Apple atom Management Security Services Configuration Security Service Security Service Security Service Melific and Activity Acti Service Security Service Configuration Security Public Acti Service Security Service Configuration Security Public Acti Service Configuration Security Public Acti Service Configuration Security Public Acti Service Configuration Security Public Configuration Security Security Security Security Security S	Manage Service Setup Configuration Configuration Security Service Anti-Servare Weinfiles and Actives Decryption Eact-Application Management Profile Configuration Security Service Configuration Configuration Security Service Configuration Configuration Profile Configuration Configuration Profile Configuration Configuration Profile Configuration Config	Manage Profile Groups Service Setup * Security Jendes scart traffic exacting security profile scare security relations * Security Services * Security Mercy * Anti-Seyware * Weershilty Profession * Weershilty Profession * WileFiles and Acthorus * DRS Security * UEL Access Management * File Booking * Manage * Manage * Security Services * Manage * Security Services * Main Security Protection * Waterability Protection *	Service Setup Configuration Configuration <thconfiguration< th=""> <thconfiguration< t<="" th=""><th>Manage Profile Groups Mobile Users Service Setup • Main Service • Service Setup •<!--</th--><th>Manage Profile Groups Mobile Users • Service Setup • Configuration • Security profile scan ratific for theran, and a profile group is a solution of each indicate security profile scan ratific for theran, and a profile group is this head and a control is indicate security profile scan ratific for theran, and a profile group is this head and a control is indicate security profile scan ratific for theran, and a profile group is this head and a control is indicate security profile scan ratific for theran, and a profile group is this head and a control is indicate security profile scan ratific for theran, and a profile group is this head and a control is indicate security profile scan ratific for theran, and a group is the head and a control is indicate security profile. Security Services • Weile Security • Security Services • Weile Security • Weile Security • Security Services • Security Services</th><th>Markage Profile Groups Mobile Users Service Setup • Configuration • Security Services • Security Services • Security Services • Security Services • Were ability Protection • Security Services • Were ability Protection • Security Service • Profile Groups • Security Service • Profile Group • Security Service • Security Service • <t< th=""><th>Markage Profile Groups Mobile Users Service Setup • Service Setup •</th><th>Manage Profile Groups (Mobile Users) Service Setup Configuration Video addition and Activities Name Service Setup Name User addition and Activities Name Service Setup Configuration Service Setup Configuration Service Setup Configuration Service Setup Configuration Service Setup Profile Group Service Setup Profile Group Service Setup Profile Group Service Setup Name Service Setup Name Service Setup Name Name</th><th>Manage Profile Groups (Mobile Users) Service Setup Incritive profiles scarving reasonabilities profile groups in submitties on the same region of profiles (Security Profile Groups (Security Profile Group) (Security Profile Groups (Security Profile Group (Security Profile Group (Security Profile Group) (Security Profile Groups (Security Profile Group) (Security Profile Groups (Security Profile Group) (Security Profile Groups (Security Profile Group) (Security Profile (Security Prof</th><th>Service Setup Profile Groups (Mobile Users) Service Setup Corringuration Value-calify Protocolory Corringuration Value-calify None of the setup setup</th></t<></th></th></thconfiguration<></thconfiguration<>	Manage Profile Groups Mobile Users Service Setup • Main Service • Service Setup • </th <th>Manage Profile Groups Mobile Users • Service Setup • Configuration • Security profile scan ratific for theran, and a profile group is a solution of each indicate security profile scan ratific for theran, and a profile group is this head and a control is indicate security profile scan ratific for theran, and a profile group is this head and a control is indicate security profile scan ratific for theran, and a profile group is this head and a control is indicate security profile scan ratific for theran, and a profile group is this head and a control is indicate security profile scan ratific for theran, and a profile group is this head and a control is indicate security profile scan ratific for theran, and a group is the head and a control is indicate security profile. Security Services • Weile Security • Security Services • Weile Security • Weile Security • Security Services • Security Services</th> <th>Markage Profile Groups Mobile Users Service Setup • Configuration • Security Services • Security Services • Security Services • Security Services • Were ability Protection • Security Services • Were ability Protection • Security Service • Profile Groups • Security Service • Profile Group • Security Service • Security Service • <t< th=""><th>Markage Profile Groups Mobile Users Service Setup • Service Setup •</th><th>Manage Profile Groups (Mobile Users) Service Setup Configuration Video addition and Activities Name Service Setup Name User addition and Activities Name Service Setup Configuration Service Setup Configuration Service Setup Configuration Service Setup Configuration Service Setup Profile Group Service Setup Profile Group Service Setup Profile Group Service Setup Name Service Setup Name Service Setup Name Name</th><th>Manage Profile Groups (Mobile Users) Service Setup Incritive profiles scarving reasonabilities profile groups in submitties on the same region of profiles (Security Profile Groups (Security Profile Group) (Security Profile Groups (Security Profile Group (Security Profile Group (Security Profile Group) (Security Profile Groups (Security Profile Group) (Security Profile Groups (Security Profile Group) (Security Profile Groups (Security Profile Group) (Security Profile (Security Prof</th><th>Service Setup Profile Groups (Mobile Users) Service Setup Corringuration Value-calify Protocolory Corringuration Value-calify None of the setup setup</th></t<></th>	Manage Profile Groups Mobile Users • Service Setup • Configuration • Security profile scan ratific for theran, and a profile group is a solution of each indicate security profile scan ratific for theran, and a profile group is this head and a control is indicate security profile scan ratific for theran, and a profile group is this head and a control is indicate security profile scan ratific for theran, and a profile group is this head and a control is indicate security profile scan ratific for theran, and a profile group is this head and a control is indicate security profile scan ratific for theran, and a profile group is this head and a control is indicate security profile scan ratific for theran, and a group is the head and a control is indicate security profile. Security Services • Weile Security • Security Services • Weile Security • Weile Security • Security Services • Security Services	Markage Profile Groups Mobile Users Service Setup • Configuration • Security Services • Security Services • Security Services • Security Services • Were ability Protection • Security Services • Were ability Protection • Security Service • Profile Groups • Security Service • Profile Group • Security Service • Security Service • <t< th=""><th>Markage Profile Groups Mobile Users Service Setup • Service Setup •</th><th>Manage Profile Groups (Mobile Users) Service Setup Configuration Video addition and Activities Name Service Setup Name User addition and Activities Name Service Setup Configuration Service Setup Configuration Service Setup Configuration Service Setup Configuration Service Setup Profile Group Service Setup Profile Group Service Setup Profile Group Service Setup Name Service Setup Name Service Setup Name Name</th><th>Manage Profile Groups (Mobile Users) Service Setup Incritive profiles scarving reasonabilities profile groups in submitties on the same region of profiles (Security Profile Groups (Security Profile Group) (Security Profile Groups (Security Profile Group (Security Profile Group (Security Profile Group) (Security Profile Groups (Security Profile Group) (Security Profile Groups (Security Profile Group) (Security Profile Groups (Security Profile Group) (Security Profile (Security Prof</th><th>Service Setup Profile Groups (Mobile Users) Service Setup Corringuration Value-calify Protocolory Corringuration Value-calify None of the setup setup</th></t<>	Markage Profile Groups Mobile Users Service Setup • Service Setup •	Manage Profile Groups (Mobile Users) Service Setup Configuration Video addition and Activities Name Service Setup Name User addition and Activities Name Service Setup Configuration Service Setup Configuration Service Setup Configuration Service Setup Configuration Service Setup Profile Group Service Setup Profile Group Service Setup Profile Group Service Setup Name Service Setup Name Service Setup Name Name	Manage Profile Groups (Mobile Users) Service Setup Incritive profiles scarving reasonabilities profile groups in submitties on the same region of profiles (Security Profile Groups (Security Profile Group) (Security Profile Groups (Security Profile Group (Security Profile Group (Security Profile Group) (Security Profile Groups (Security Profile Group) (Security Profile Groups (Security Profile Group) (Security Profile Groups (Security Profile Group) (Security Profile (Security Prof	Service Setup Profile Groups (Mobile Users) Service Setup Corringuration Value-calify Protocolory Corringuration Value-calify None of the setup

Click Save to accept changes.

• Required Field

Navigate to Security Policy > under the Mobile Users > Rulebase tab, add or edit the existing policy; if the intent is to enforce the web isolation for a particular set of users, add the proper users under the Source tab.

4	Manage	Manage >							Push Config *
•	Service Setup *			Policy Mobile Users -	resou	rcei to enhancing ;	productivity and effici	ency.	
0	Configuration *	Rulebase	De	d Practions					
	Security Services								
2	Security Policy	-							
а	Anti-Spyware	U,	vad Ne	se Filter					Reset Filters
	Vulnerability Protection	Securi	ty Po	ficy Rules (15) Q. Searth		C Panta		Cheve Mary	Autor
۰.	WildFire and Antivirus	and the second		and server (1994) and a server		U .			
	DNS Security								
	URL Access Management File Blocking			Name		BPA Verdet	Cleanup	Zone	Address
	HTTP Header Insertion	· Pris	na Acc	ons - Pro Rules (E)					
	Profile Groups		1	Allow All		O Fail		trust	aw
	SaaS Application Management		2	Drop Traffic to Known Malicinus IP Addresses	-	Pass	Zero Hit Rule	300	are
	Decryption		4	propriate to known manolitis in Addresses	-	V 7800		any	114
	Network Services 9					-	Zero Hit Otja		
	Identity Services +		3	Drop Traffic to Potential High Risk IP Addresses		O Pass	Zero Hit Rule	any.	any .
	Objects +						Zero-Hit Obje		
			4	Drop Traffic to Bulksproof hosting providers		Pana	Zero-Hit Rule	any	any

Under the *Service Entities*, set the services as **Any Service** (don't use the **application-default** as the redirection might involve non-standard ports).

4	Manage	Manage 3 Security Policy 3 Security Policy Rule - Mobile Users	
•	Service Setup +	Add Security Policy Rule	III Best Practice Checks
•	Configuration Security Services Security Palicy	Applications, Services and URLs Control applications, services (protocol and port-usage), and web access based on URL categories. APPLICATION ENTITIES * Any Application	
•	Anti-Spyware Wulnerability Protection WildFire and Antivirus	Add Applications Add Application Groups Add Application Filters	
	DNS Security URL Access Management File Blocking HTTP Header Insertion	SERVICE ENTITIES * Any Service ~ Add Services Add Service Groups	
	Profile Groups SaaS Application Management Decryption	URL CATEGORY ENTITIES Any URL Category Add URL Categories Add External Dynamic Lists	
*	Network Services v Identity Services v	Add SaaS Application Endpoints	
?	Objects 👻	TENANT RESTRICTIONS Add SadS Applications	

Under the *Action and Advanced Inspection* section, select the **Allow** option. Under the Profile Group, select the Profile Group defined in the previous step.

4	Manage	Manage > Security Policy > Securit			
•	Service Setup -	Add Security Policy F	Rule		III Best Practice Checks
0 0 1 1	Configuration Security Services Security Policy Anti-Spyware Uninerability Protection WildFire and Antivirus DNS Security URL Access Management File Blocking HITTPHeader Insertion Profile Groups	Action and Advanced I Set the action to take on traffic that m gradice security profile settings. Action * Allow Sendi ICMP Unreachable Profile Group Menio Security Profile Anti-Spynare	-	cified above. By default, this traffic i	s also scanned for threats based on the best
? · ·	SaaS Application Management Decryption Network Services • Identity Services • Objects •	Vulnerability Protection URL Access Management File Blocking HTTP Header Insertion WildFire and Antivirus • Required Field	Menia-Security		Cancel Son

Click Save to confirm changes. Then click Push Config and Push to apply the changes.

Continue with the common Step 4 and Step 5 further in this document.

3.3. Transparent redirection with Prisma Access Traffic Steering

Step 1: Configure an IPsec Tunnel connecting to the Menlo Security cloud

Contact Menlo Security and request the provisioning of an IPSec tunnel pair.

Important You need to provide Menlo Security Customer Success with your service IP address so the IPsec tunnel pair can be created.

Obtain the below information from Menlo Security for each tunnel to setup the IPSec tunnels on the Prisma Access side:

- Gateway IP address
- Pre-shared Key
- Peer Identifiers
- Tunnel IP Address

Navigate to *Manage > Service Setup > Service Connections* and create a new Service Connection that will link the Prisma Access instance to the Menlo Secure Cloud Browser.

٠	Manage Investment -		Nee 9 Interference 9 Interference Naté Service Connection								
	hHH	General 	na.e		landa Manan						
	Testigonite 1	- Prinary Tarvel			1 a ¹⁶ 0 ¹⁶ 1 a 16						
		Ruling					94		200		
				00				0.9			

Select a **Prisma Access Region** and **Location** as close as possible from the majority of the users that will be redirected to Menlo Security. If the users are geographically dispersed, multiple Service Connections would be recommended for a better user experience.

Step 2: Select the proper IKE crypto and IPSec crypto settings

Under the Primary Tunnel Setup menu, use the settings captured below as an example:

Note

Enabling **Tunnel Monitoring** is recommended to monitor the status of the IPsec tunnels by passing ICMP packets through the tunnel to verify it's operational. The IP address in the range 169.254.0.0/16 is used as the destination address for tunnel monitoring. The destination address can be same if they are established with different IKE peers, otherwise it has to be unique.

Edit Menlo_W_Primary		
< Back		
Tunnel Name *		
Menlo_W_Primary		
Branch Device Type		
Other Devices		*
Authentication		
Pre-Shared Key		
Pre-Shared Key 🏶		
•••••	•••••	
Confirm Pre-Shared Key *		
•••••	•••••	
IKE Local Identification FQDN (hostname)	× v	Prisma_Tunnel_16_1
IKE Peer Identification		
FQDN (hostname)	X¥	Menlo_16_Primary
Branch Device IP Address		
Static IP O Dynamic		
Static IP *		
54.		
IKE Passive Mode		
INC FOSIVE MODE		
Turn on Tunnel Monitoring		
Destination IP *		

Under the IKE Advanced Options select the following combinations:

IKE Advanced Options	
< Back	
IKE Protocol Version	
IKEv2 only mode	× •
IKEv2 Crypto Profile	
Menlo_Security_IKE	× •
Create New Manage	
IKE NAT Traversal	
	Cancel Save

Note

The **Lifetime** value entered should match the Lifetime value provided by Menlo Security Customer Success for both IKE crypto and IPsec crypto settings when the IPsec tunnel is configured.

Edit Menlo_Security_IKE			
K Back			
Name *			
Menlo_Security_IKE			
Encryption * aes-128-cbc ··· +			
Authentication * sha256 ··· +			
DH Group * group19 ··· +			
Lifetime			
3	Hours		1 ₆₄ 1
IKEv2 Authentication Multiple			
0 [<= 50]			
* Required Field		Cancel	Save

Under the IPSec Advanced Options, select the following combination:

IPSec Advanced Options	
< Back	
IPSec Crypto Profile	
Menlo_Security_IPSec	× •
Create New Manage	
🛃 Anti Replay	
Copy ToS	
Enable GRE Encapsulation	
	Cancel Save

Edit Menlo_Security_IPSec		
< Back		
Name *		
Menio_Security_IPSec		
IPSec Protocol		
ESP		~
Encryption *		
aes-128-cbc … 🛉		
Authentication *		
DH Group		× •
group19		~ ~
Lifetime *		
1.5	Hours	~
Lifesize		
[1 - 65535]	MB	v
* Required Field		Cancel Save

Push the new configuration.

Once the Service Connection is created, a dedicated Public IP will get assigned; this will be the IPsec tunnel end point on the Prisma Access side; this IP can be seen under the Service IP column and will be required to be shared with Menlo Security.

	Hanage	these it into Large	Aur 2 Interferences								
*	briesbear -	fands constant nate to	envice Connections Settup type descent with copy in our tools and without advanced induced in your off to this action								-
1		Service Lorence	1.00						-		the set of the set of the
			54		Rose .		the second second				
-	Resolution II	C 944	35545	Tatast	Condig.	toote-	Tervice IP	007840	807.04	8977-0	Plac have
۰.		C Market		8-04	6 mars	Ve Grenet	URDERSON AND	1051403014	disable	Enabled	Secondary for the second

Note The IP in the image above is only one random example.

Once the IPSec tunnel is provisioned by Menlo Security as well, validate the Tunnel status turns into the Green/OK state.

Repeat the tunnel creation process for the Secondary Tunnel

For high availability, fault tolerance, and seamless service upgrades, please configure the Prisma Secondary Tunnel in the service connection. The secondary tunnel will use new addresses, peer identifiers, and pre-shared keys, which are supplied by Menlo Security Support. But the secondary tunnel will use the same Prisma Service Connection IP Address.

General				
* Name	Prod_GW			
	ingion	Location		
Prisma Access Location	North America 🛛 👻	US West	~	
Primary Tunnel				() ER
IPses Turnel	Marke W Primary			
Branch Device IP Address	54.			
Authentication	Pro Shared Key			
Tannel Manitaring IP	169.254.10.1			
Secondary Tunnel				(t) Let
IPsec Turnel	Merilo_Secondary			
Branch Device IP Address	52.			
Authentication	Pre-Shared Key			
Tunnel Monitoring IP	169.254.11.1			

Step 3: Configure the Traffic Steering rules to select what traffic is required for Isolation

Under the same Service Connections menu, select the Advanced Settings tab.

	Harage	-temp 2 toris Com	a disat								Partitively -
Ĩ	bertochelan -	Terroristication and an and	ections Setup	et alaste i suo chario e	an 17 a 18 a 19						0 mounting
	Constanting of	Senice Couned	iven 11						anymouth B		and for our discussion.
1			-		2004		Wanty Room				page 1
	Risk Chinese	100	tabuti-	frond	10/10	00080	Solut.	1007 8440	307 mu	407.014	When Party
1		U Head		6 14	0+m	different	DEDRIGATIN	PERMIT	Challer	Dates	Search 4

Under the *Traffic Steering* menu, create a new Traffic Forwarding rule.

half's Fare	varding Tuko	m.					Contract Contract	Case Man 14
			20x01		Deditoritor			
	Here	Use Betties	Address Briddes	Destination	URL Calegory	Arries	larvice .	Taypri Group
6 1	Diversion NAME	-	-	-	Printa Service Danales, respect.	Personal to the Larget	service https://www.ior.it/ips	Maria 801

Select the matching criteria for the traffic that needs to be transparently redirected through Isolation; typically the criteria are a combination of selected users and/or URL Categories.

Edit Menlo RBI		
Name *		
Menio RBI		
Source		
User Entities		
Match Any User 😒		
Source Address Entities *		
any		~
Destination		
Destination Address Entities		
any		~
URL Category		
v		
URL Category		
Menlo Service Domains ··· social-networking ··· Isolated Domains ··· unknown ··· +		
Service		
Service *		
×		
Services		
service-http ··· service-https ···		
Action		
Forward to the target Forward to the internet		
Target Service Connection Group *		
Menie RBI		~
Create New Manage		
	Cancel	Save

Name	Description
Menio Service Compins	
Custom URL Category * Type	
URL Life Matches any of the following URLs, domains or heat names.	Items (1) Q San Driver Add Faport Import Ust *menloescurity.com
	Enter one entry per row. Each entry may be of the form www.example.com it could have wildcards like www.".com.

Note that one of the redirected URL Categories is a custom URL Category that we named Menlo Service Domains and contains a wildcard for any URLs under the menlosecurity.com domain.

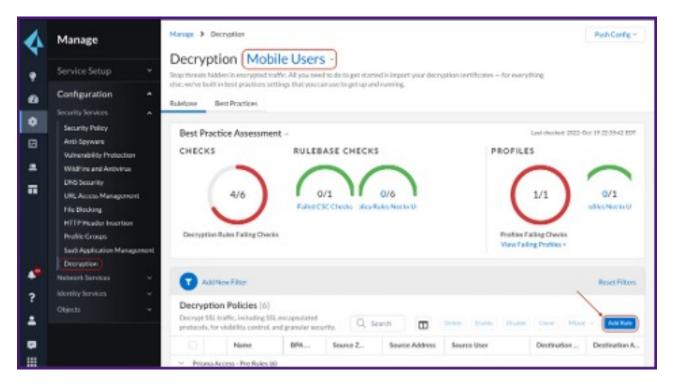
Make sure that all the above configurations are being pushed.

3.4. Common Steps for any of the selected integration methods

Step 4: Enable SSL decryption for enhancing the URL Categorization rate

Navigate to Configuration > Security Services > Decryption under the Mobile Users context.

Create a policy decrypting all the traffic for the required users.



Add the Address object that was created earlier.

4	Manage	Manage > Decryption > Decryption Palicy-Mubile Users	
	Service Setup 👻	Add Decryption Policy	IE Best Practice Checks
€ 0	Configuration Security Services Security Policy Acti-Spyware Valversbillty Protection	Source Enforce traffic based on its origin. ZONES Custom ~ Zones	
•	WildFire and Autovirus DNS Security URL Access Management File Blocking HETFHousian Insertion Profile Groups	ADDRESSES + Conten v Match Codule (Negate) Addresses Menio, Address	
* ? 4	SeeS Application Management Deception Network Services v Identity Services v Objects v	Add Address Groups Add External Dynamic Lists Add Regions USERS = Any Uner ~ Add User Groups Add Users	
•		# Required Field	Cancel Ser

Click the Push Config button and Push.

Step 5: Verify the redirection works as expected

Connect a Mobile User to the Prisma Access instance via the GlobalProtect client.

Try to access any URL under the categories selected for redirection.

The user should be prompted to authenticate against the Menlo Security solution; after the user is passing the authentication once, other further redirections to Menlo Security will not require the authentication step anymore.

Note

In the case of the Transparent Redirection method, the original URL that is being accessed by the user remains unchanged (no prepend). This makes the user experience in this case totally transparent for the URLs accessed through Isolation.

4. Menlo Security Configuration

The first two integration methods are using the 'prepend' mode in the Menlo Security solution (prepending safe.menlosecurity.com in front of the original URL). This mode will automatically trigger an Isolate action on the Menlo Security so there is no specific configuration required on the Menlo Security side.

The transparent redirection integration methods leave the original URL that the user is accessing unchanged. For this integration method, ensure that all URL categories and Threat types have the "Isolate" or "Isolate Read-Only" action selected in *Web Policy > Categories / Threats*. This policy ensures that any traffic selected by the Prisma forwarding policy will be isolated by the Menlo Security platform.

MERLS Policy				III 🛞 🔇
WH -	Web - Catoparies			Form I Publis
DEM. POLICY	 Interference 	C BOB'S	*	
Decals	 Military 	isolatia		
Categorian	Motor Whiteles	O isolata		
baoureens / Archives	L Music	🔿 isolatia	•	
No lip-back	Nova and Media	O Isolete	-	
071005	Nully	Q Isolate	-	
98. Decryption Dosmptions oficy Exceptions	Online Densting cards	O hoolante	.*	
-10423	Open HTTP Proces	O toolarte	*	
Contrast traject ion	Payto Suf	O tookra		
Applications +	Peer to Peer	C isolars	*	

5. Troubleshooting

In case of issues, the traffic should be tracked step by step, first by checking if Prisma Access is applying the expected action to the desired traffic. We can verify this by looking into the *Logs* > *Firewall/URL logs*.

ACCESS	Logs Your high any automatically generated and pr logs report all points where Prima Arrays	oude ar audit Gall for system, surdiguistics, a muse tene astronol softe	of Actuarts marrie. Naturesh				
🕈 kogito 🔹 k							_
Actoremous DDH +	Perestal	top party				-	
🗴 Hanage 💿 🔹				03/00/0811 10/2410	PM -36/20/2021 30/2100 PM 1	1.575.074-mult	Tage Miles 1271
Million	Time Generated 1	URL .	URL Domain	WitCompry	Mic Gatapry Litr	Snedy	Hore Zow
Exports	(*) 64/07/0011 (2113/2 ¹⁷ Her H)T	endpointingness-salif-com/	endpoint.ingrou.rs	Spe-SA	computer and internet in		Part

The next place to check is in the Menlo Security platform logs to confirm that the traffic is Isolated as expected.

5.1. Technical Support

- · Contact information for Palo Alto technical support: https://support.paloaltonetworks.com
- Contact information for Menlo Security technical support: https://csportal.menlosecurity.com