

# Palo Alto Prisma Access: Cloud Managed Integration Guide

Applies to: Menlo Cloud  
Version Information: 2.86  
Date Updated: October 2022

<b>Revision History</b>	<b>2</b>
<b>Use Cases for Integration with Palo Alto Prisma Access Simplify User Policy Enforcement</b>	<b>3</b>
Challenge	3
Solution	3
Protecting High-Risk Users and Applications	3
Challenge	3
Solution	3
<b>Integration Benefits</b>	<b>4</b>
<b>Integration Diagram</b>	<b>4</b>
<b>Before You Begin</b>	<b>5</b>
<b>Palo Alto Networks Configuration</b>	<b>5</b>
Method 1A. Block action integration method	6
Method 1B. Override action Integration method	10
Configuration for both Block and Override modes	13
Method 2. Transparent redirection with Prisma Access Traffic Steering	16
Common Steps for all integration methods	25
Menlo Security Configuration	29
Troubleshooting	30

## Revision History

Release	Date	Change
2.86	October 2022	Initial Release

# Use Cases for Integration with Palo Alto Prisma Access Simplify User Policy Enforcement

## Challenge

The internet contains more than 4 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 Security Isolation Platform 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 Security Isolation Platform. 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

## 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 Security Isolation Platform via integration with Prisma Access. This ensures that any website the specified user or group accesses is executed within the cloud-based Menlo Security Isolation Platform, 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 Security Isolation Platform 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.

## Integration Benefits

Palo Alto Prisma Access and the Menlo Security Isolation Platform 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.

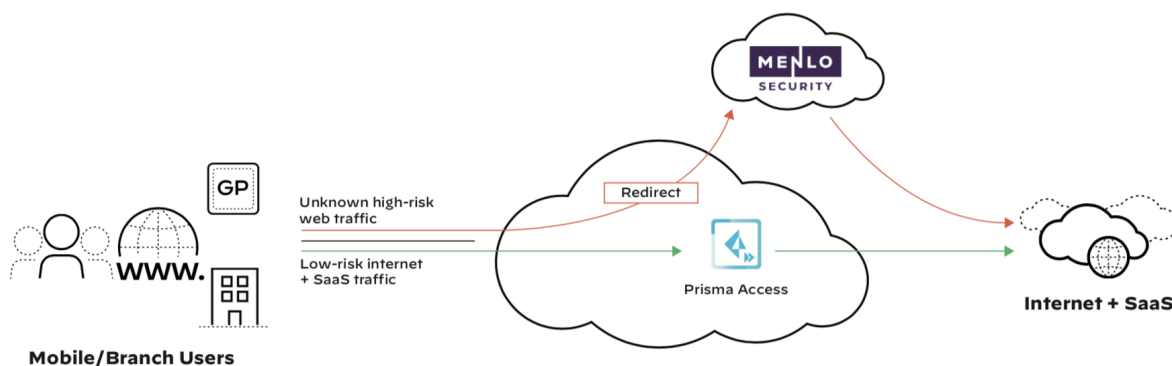
Complies with regulations for air-gapping high-value users.

Improves user productivity, unhindered by excessive website blocks.

Reduces help desk tickets from users whose access to websites has been blocked. Combines the benefits of Palo Alto Prisma Access policy and Isolation

## Integration Diagram

As covered in the use-cases description above, specific Internet and SaaS traffic defined by the use-case criteria (certain users, certain URLs or any combination of both) is redirected to the Menlo Security solution; this to introduce the air-gap offered by the web-isolation:



**Figure 1:** Forwarding of specific traffic to Menlo Security for browser isolation



## Before You Begin

To ensure a smooth configuration process, please ensure the following prerequisites are met:  
Access to the Prisma Access instance and the Panorama instance 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](https://admin.menlosecurity.com))

## Palo Alto Networks Configuration

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

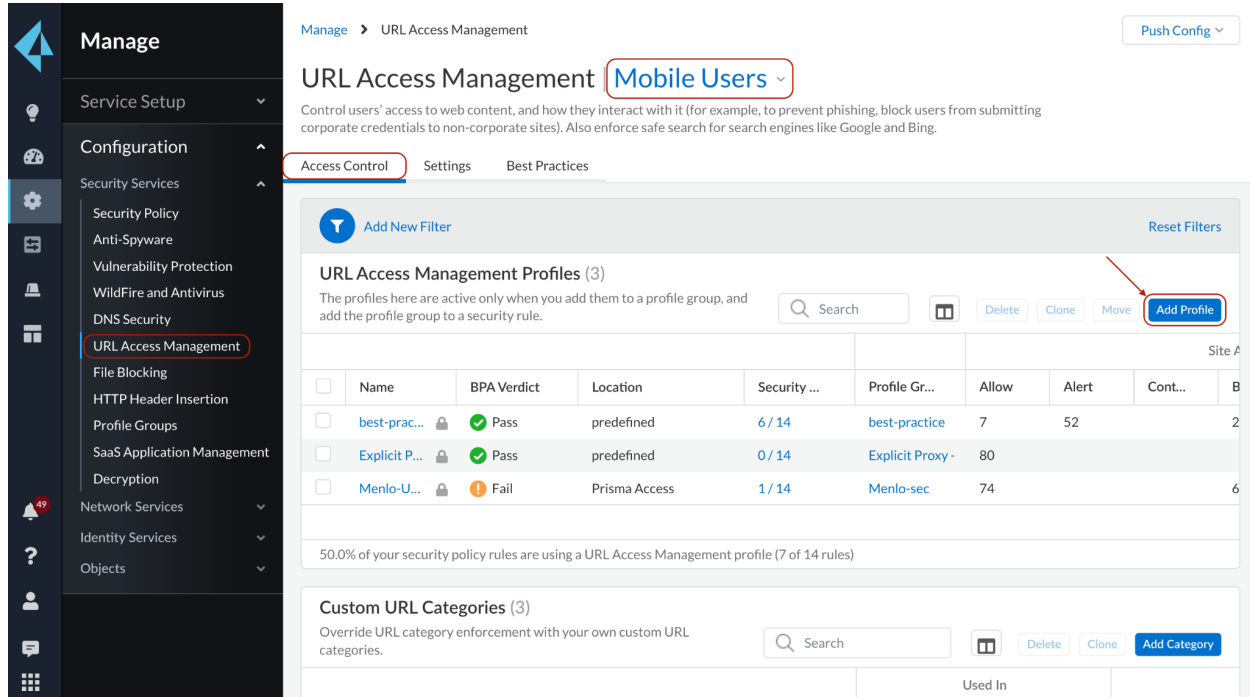
1. Using categorization to redirect web requests to “prepend” isolation mode. This can be done two ways
  - a. by a “block” “ action set to the desired URL Category and a custom Block Response Page.
  - b. by an “override” action set to the desired URL Category, that can later be applied to a Security 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

The configuration details are covered below.

## Method 1A. 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



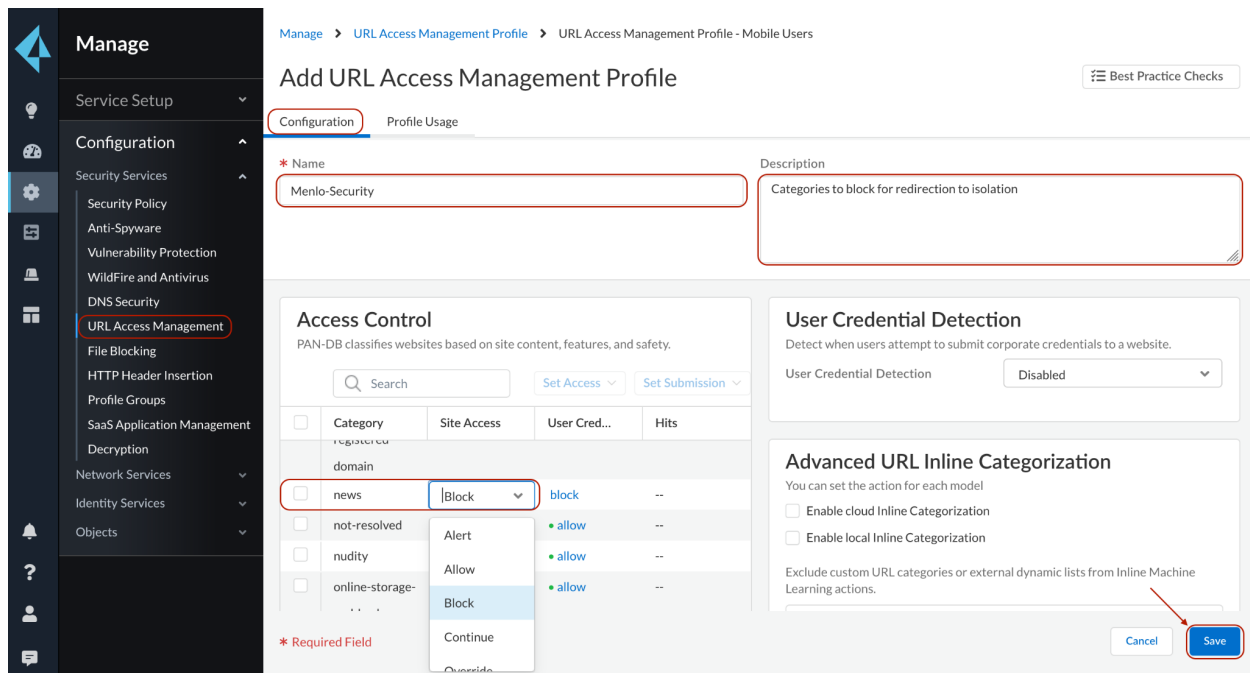
The screenshot shows the Prisma Access Cloud Management portal interface. On the left is a dark sidebar with a 'Manage' header and a list of configuration options. The 'URL Access Management' option is highlighted with a red box. The main content area shows the 'URL Access Management' page for the 'Mobile Users' context. The 'Access Control' tab is selected. Below the tabs, there is a section for 'URL Access Management Profiles (3)' with a table listing profiles. The 'Add Profile' button is highlighted with a red box and an arrow. Below the profiles table, there is a section for 'Custom URL Categories (3)' with a table listing categories.

Name	BPA Verdict	Location	Security ...	Profile Gr...	Allow	Alert	Cont...	Site A
best-prac...	Pass	predefined	6 / 14	best-practice	7	52		2
Explicit P...	Pass	predefined	0 / 14	Explicit Proxy -	80			
Menlo-U...	Fail	Prisma Access	1 / 14	Menlo-sec	74			6

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:



Manage > URL Access Management Profile > URL Access Management Profile - Mobile Users

## Add URL Access Management Profile

Best Practice Checks

**Configuration** Profile Usage

\* Name: Menlo-Security

Description: Categories to block for redirection to isolation

**Access Control**  
PAN-DB classifies websites based on site content, features, and safety.

Search: [ ] Set Access: [v] Set Submission: [v]

Category	Site Access	User Cred...	Hits
news	Block	block	--
not-resolved	Alert	allow	--
nudity	Allow	allow	--
online-storage-	Block	allow	--

\* Required Field

**User Credential Detection**  
Detect when users attempt to submit corporate credentials to a website.  
User Credential Detection: Disabled

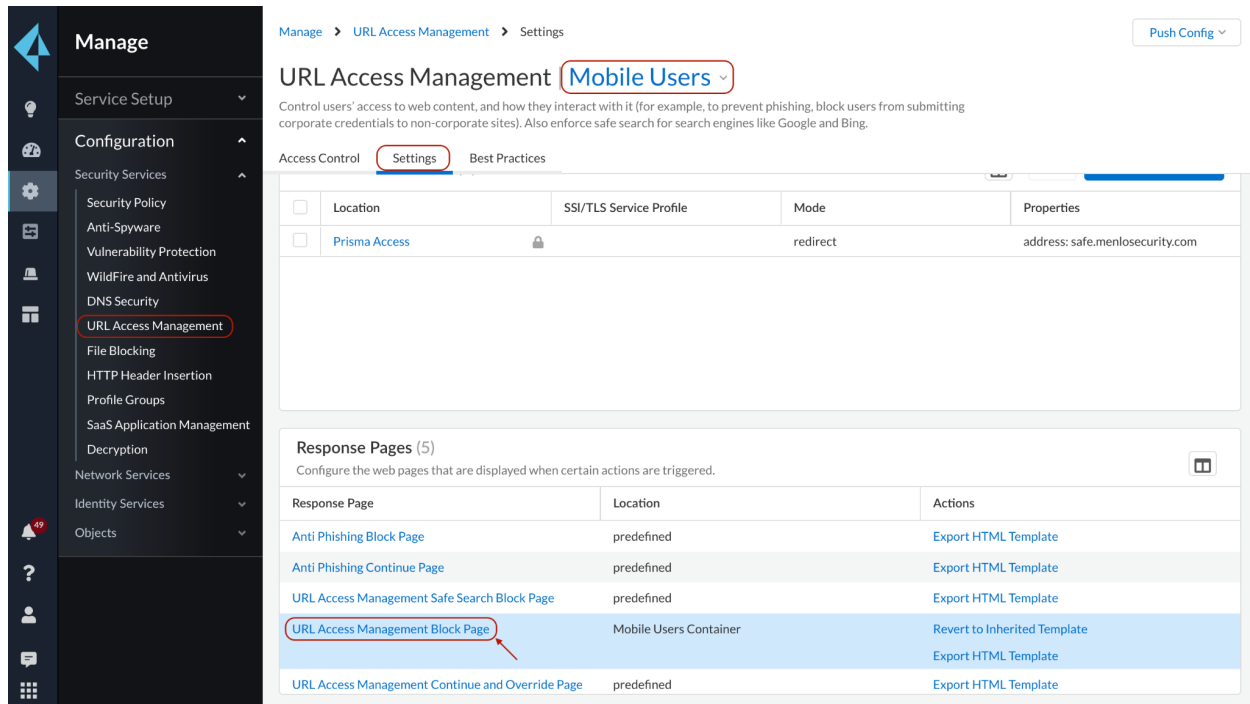
**Advanced URL Inline Categorization**  
You can set the action for each model  
☐ Enable cloud Inline Categorization  
☐ Enable local Inline Categorization  
 Exclude custom URL categories or external dynamic lists from Inline Machine Learning actions.

Cancel Save

## 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”



Manage > URL Access Management > Settings Push Config

### URL Access Management Mobile Users

Control users' access to web content, and how they interact with it (for example, to prevent phishing, block users from submitting corporate credentials to non-corporate sites). Also enforce safe search for search engines like Google and Bing.

Access Control Settings Best Practices

Location	SSI/TLS Service Profile	Mode	Properties
<a href="#">Prisma Access</a>		redirect	address: safe.menlosecurity.com

#### Response Pages (5)

Configure the web pages that are displayed when certain actions are triggered.

Response Page	Location	Actions
Anti Phishing Block Page	predefined	<a href="#">Export HTML Template</a>
Anti Phishing Continue Page	predefined	<a href="#">Export HTML Template</a>
URL Access Management Safe Search Block Page	predefined	<a href="#">Export HTML Template</a>
<b>URL Access Management Block Page</b>	Mobile Users Container	<a href="#">Revert to Inherited Template</a> <a href="#">Export HTML Template</a>
URL Access Management Continue and Override Page	predefined	<a href="#">Export HTML Template</a>

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

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

```
<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:1em;
  }
  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(prepend);
  }

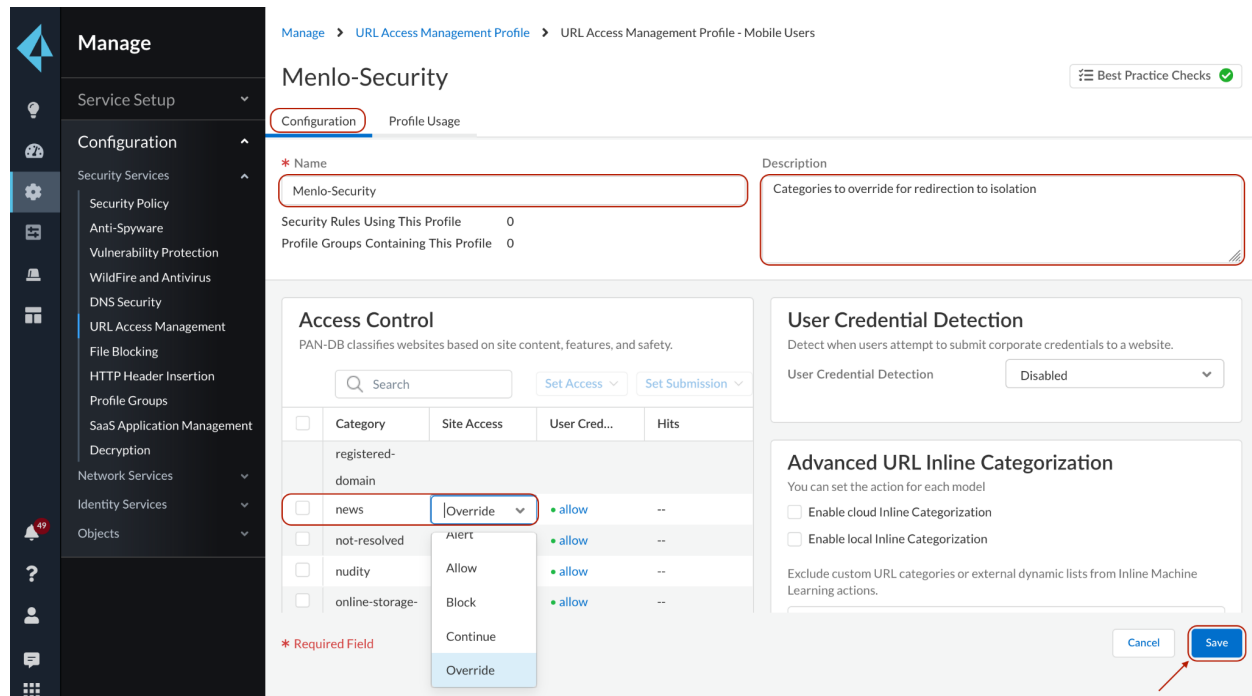
  // window.location.replace('https://safe.menlosecurity.com')
</script>
</head>
<body bgcolor="#e7e8e9">
<div id="content">
<h1>Web Page Blocked</h1>
<p>Access to the web page you were trying to visit has been
blocked in
accordance with company policy. Please contact your system administrator
if you believe this is in error.</p>
<p><b>User:</b> <user/> </p>
<p><b>URL:</b> <url/> </p>
<p><b>Category:</b> <category/> </p>
<p>To view the page in <b>Isolation</b>
</div>
</body>
</html>
```

## Method 1B. 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)



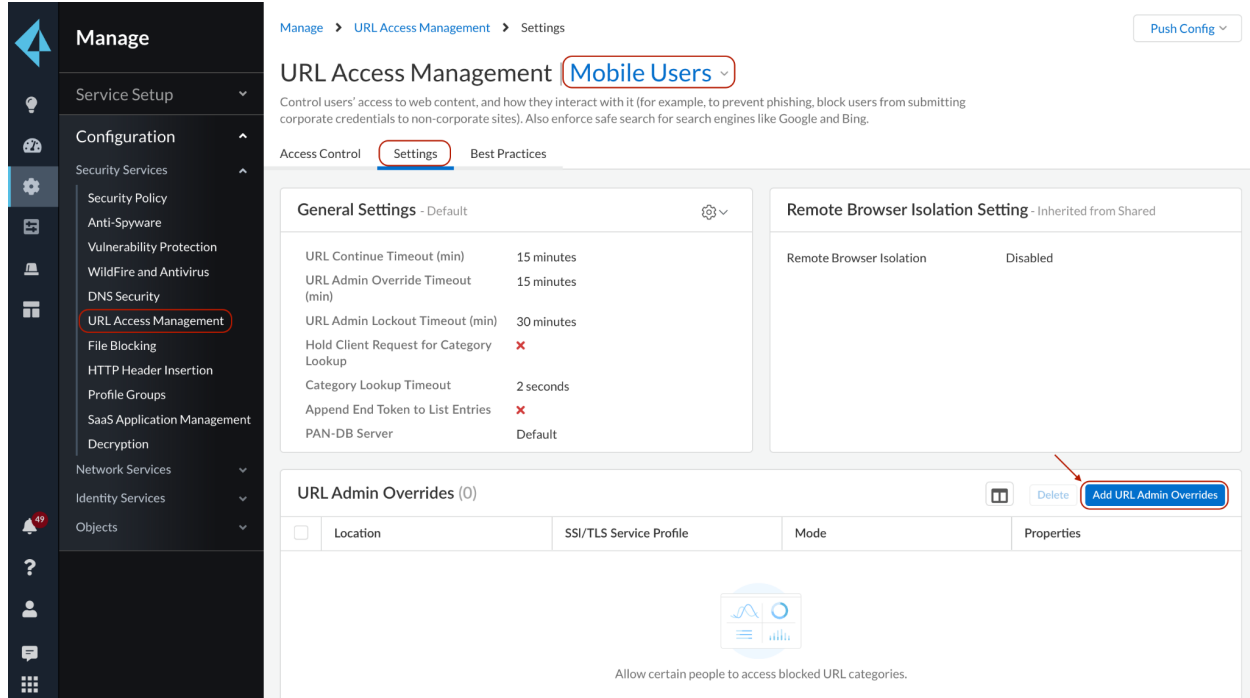
The screenshot shows the Menlo Security configuration interface. The left sidebar contains a 'Manage' section with a 'Configuration' tab selected. The main area displays the 'Menlo-Security' profile configuration. The 'Configuration' tab is active, showing the 'Access Control' section. The 'Access Control' section includes a table with columns for 'Category', 'Site Access', 'User Cred...', and 'Hits'. The 'news' category is selected, and the 'Site Access' dropdown is set to 'Override'. The 'User Credential Detection' section is also visible, showing a 'Disabled' status. The 'Advanced URL Inline Categorization' section is at the bottom, with options to enable cloud or local inline categorization. A red arrow points to the 'Save' button in the bottom right corner.

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”



The screenshot shows the Menlo Security management console. On the left is a dark sidebar with a 'Manage' section containing 'Service Setup', 'Configuration', and 'Security Services'. Under 'Configuration', 'URL Access Management' is highlighted. The main panel shows the 'URL Access Management' settings for 'Mobile Users'. The 'Settings' tab is active, displaying 'General Settings' and 'Remote Browser Isolation Setting'. At the bottom, the 'URL Admin Overrides (0)' section is visible, with a red arrow pointing to the 'Add URL Admin Overrides' button.

Manage > URL Access Management > Settings Push Config

URL Access Management **Mobile Users**

Control users' access to web content, and how they interact with it (for example, to prevent phishing, block users from submitting corporate credentials to non-corporate sites). Also enforce safe search for search engines like Google and Bing.

Access Control **Settings** Best Practices


**General Settings** - Default

URL Continue Timeout (min)	15 minutes
URL Admin Override Timeout (min)	15 minutes
URL Admin Lockout Timeout (min)	30 minutes
Hold Client Request for Category Lookup	✗
Category Lookup Timeout	2 seconds
Append End Token to List Entries	✗
PAN-DB Server	Default

**Remote Browser Isolation Setting** - Inherited from Shared

Remote Browser Isolation	Disabled
--------------------------	----------

URL Admin Overrides (0) Delete **Add URL Admin Overrides**

<input type="checkbox"/>	Location	SSI/TLS Service Profile	Mode	Properties
 <p>Allow certain people to access blocked URL categories.</p>				

In the URL Admin Override pane, click Add. In the URL Admin Override window, fill in the form fields with the following values:

- 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
- Mode: Redirect
- Address: redirector.menlosecurity.com

## URL Admin Override Settings

Mode

☐ Transparent
 ☒ Redirect

\* Address

redirector.menlosecurity.com

\* Password

.....

.....

\* Confirm Password

.....

SSL/TLS Service Profile

None

▼

Create New

Manage

\* Required Field

Cancel

Save

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

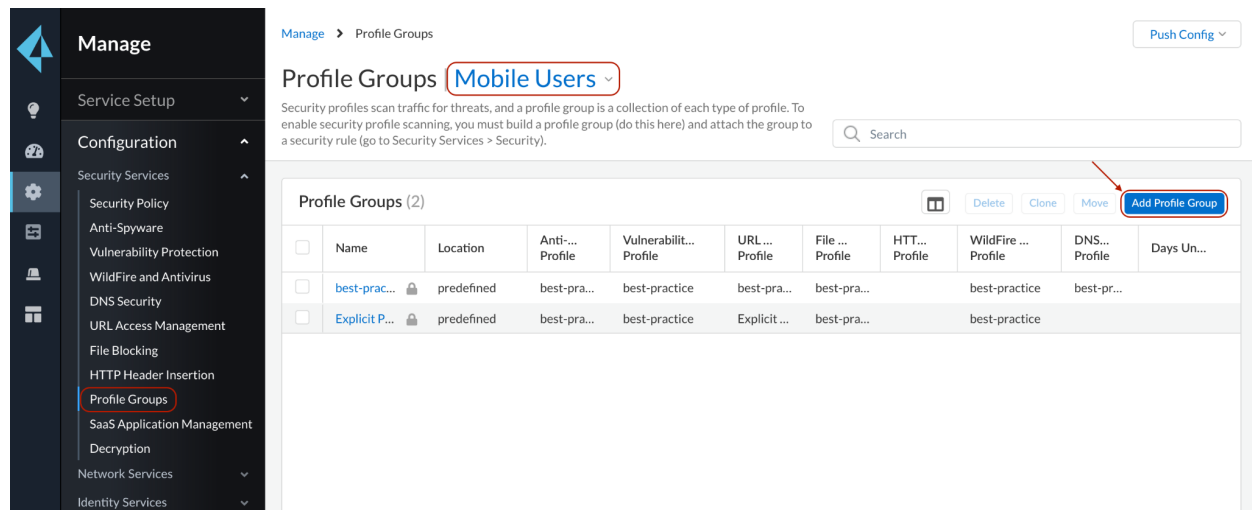


## Configuration for both Block and Override modes

### 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

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



Manage > Profile Groups

Push Config

### Profile Groups Mobile Users

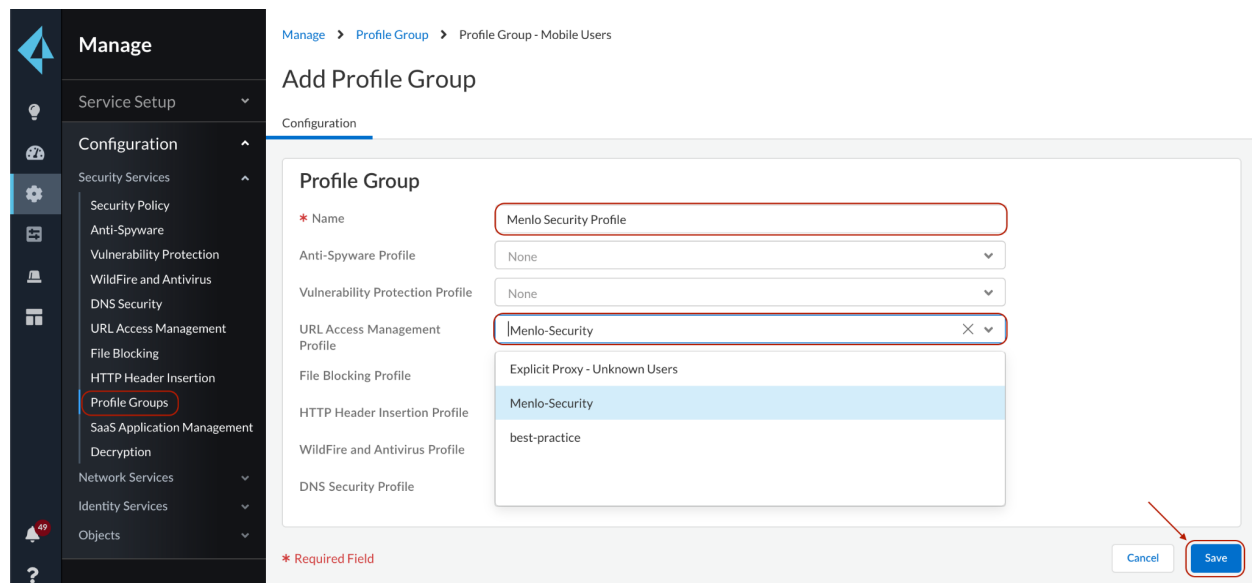
Security profiles scan traffic for threats, and a profile group is a collection of each type of profile. To enable security profile scanning, you must build a profile group (do this here) and attach the group to a security rule (go to Security Services > Security).

Search

Profile Groups (2)

	Name	Location	Anti-Spyware Profile	Vulnerability Protection Profile	URL Access Management Profile	File Blocking Profile	HTTP Header Insertion Profile	WildFire and Antivirus Profile	DNS Security Profile	Days Un...
<input type="checkbox"/>	best-prac...	predefined	best-pra...	best-practice	best-pra...	best-pra...		best-practice	best-pr...	
<input type="checkbox"/>	Explicit P...	predefined	best-pra...	best-practice	Explicit ...	best-pra...		best-practice		

Buttons: Delete, Clone, Move, **Add Profile Group**



Manage > Profile Group > Profile Group - Mobile Users

### Add Profile Group

Configuration

#### Profile Group

\* Required Field

Name: Menlo Security Profile

Anti-Spyware Profile: None

Vulnerability Protection Profile: None

URL Access Management Profile: Menlo-Security

File Blocking Profile: Explicit Proxy - Unknown Users

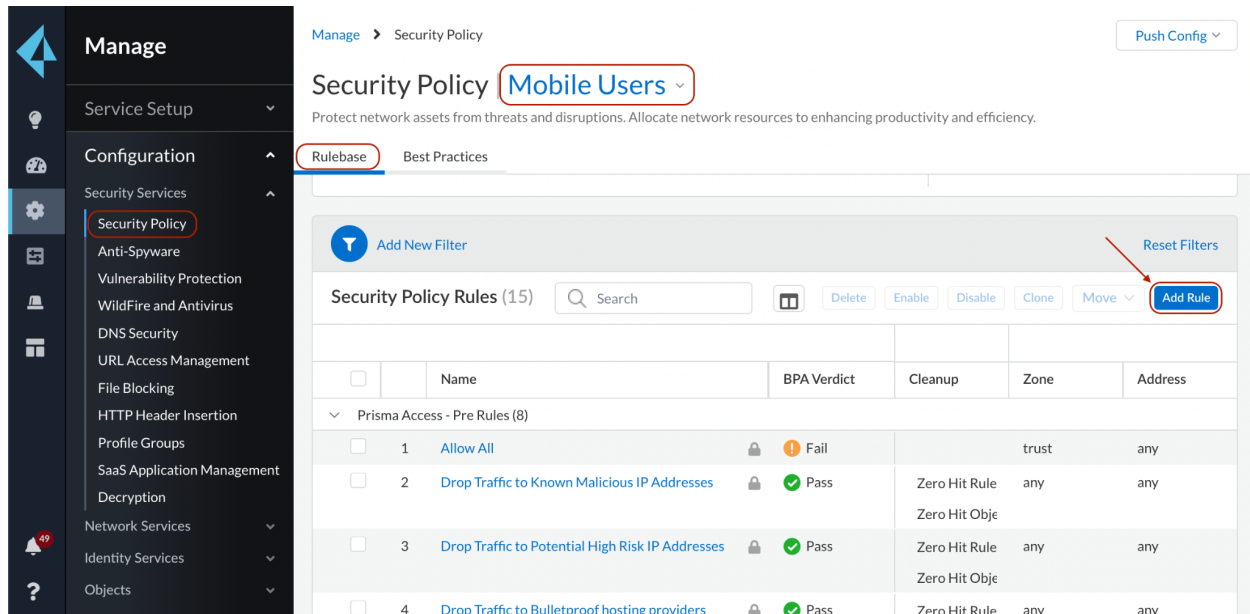
HTTP Header Insertion Profile: Menlo-Security

WildFire and Antivirus Profile: best-practice

DNS Security Profile:

Buttons: Cancel, **Save**

Navigate to Security Policy > under Mobile Users > Rulebase tab, and 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.



Manage > Security Policy

Security Policy **Mobile Users**

Protect network assets from threats and disruptions. Allocate network resources to enhancing productivity and efficiency.

Rulebase Best Practices

Add New Filter

Reset Filters

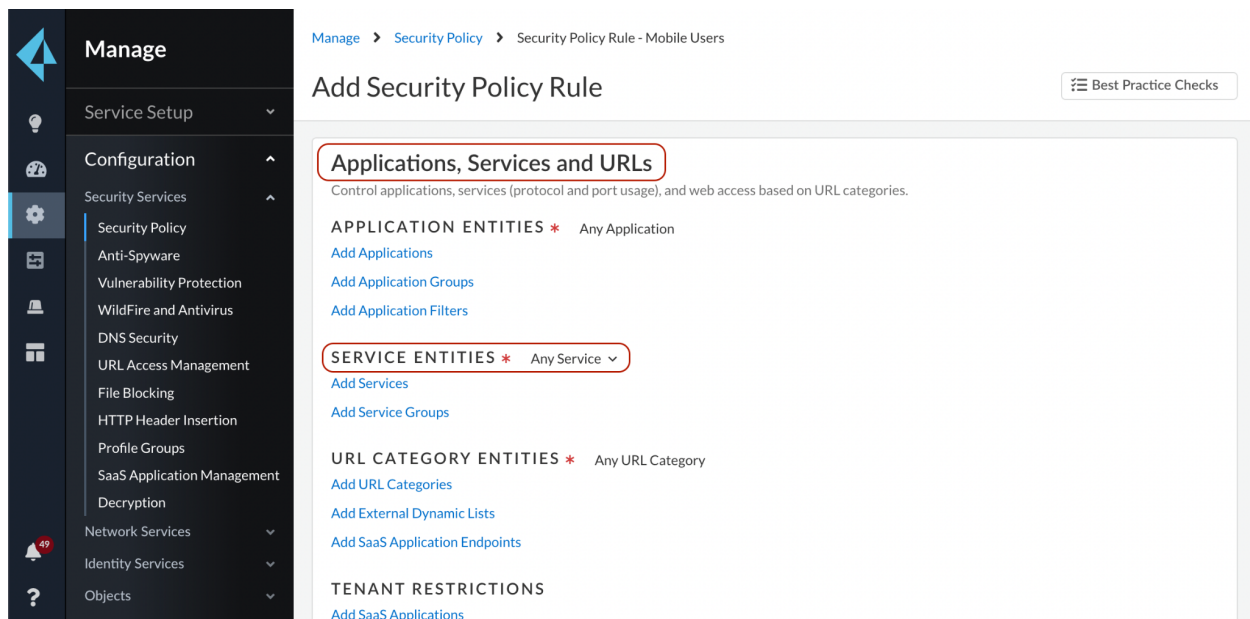
Security Policy Rules (15)

Search

Delete Enable Disable Clone Move Add Rule

	Name	BPA Verdict	Cleanup	Zone	Address
Prisma Access - Pre Rules (8)					
<input type="checkbox"/>	1 Allow All	Fail		trust	any
<input type="checkbox"/>	2 Drop Traffic to Known Malicious IP Addresses	Pass	Zero Hit Rule	any	any
<input type="checkbox"/>	3 Drop Traffic to Potential High Risk IP Addresses	Pass	Zero Hit Rule	any	any
<input type="checkbox"/>	4 Drop Traffic to Bulletproof hosting providers	Pass	Zero Hit Rule	any	any

Under the Service Entities set the services as “Any Service” (don’t use the “application-default” as the redirection may involve non-standard ports)



Manage > Security Policy > Security Policy Rule - Mobile Users

Add Security Policy Rule

Best Practice Checks

Applications, Services and URLs

Control applications, services (protocol and port usage), and web access based on URL categories.

APPLICATION ENTITIES \* Any Application

Add Applications

Add Application Groups

Add Application Filters

SERVICE ENTITIES \* Any Service

Add Services

Add Service Groups

URL CATEGORY ENTITIES \* Any URL Category

Add URL Categories

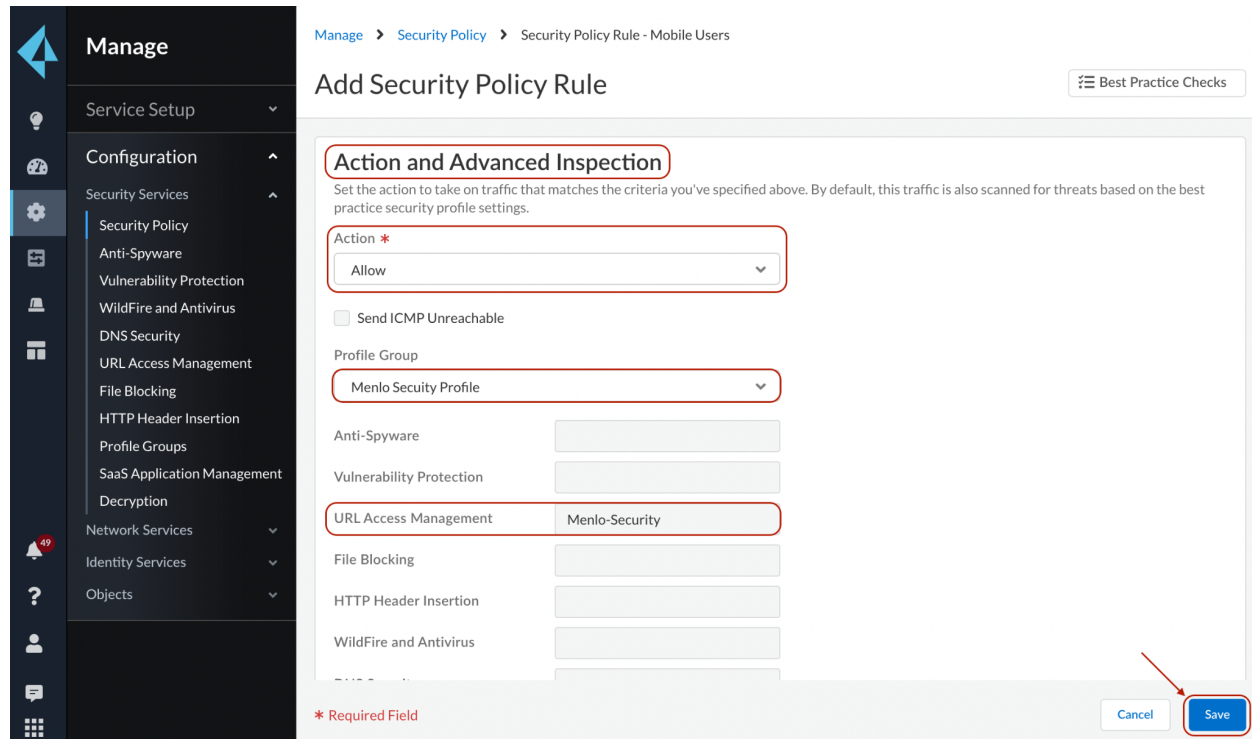
Add External Dynamic Lists

Add SaaS Application Endpoints

TENANT RESTRICTIONS

Add SaaS 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.



Manage > Security Policy > Security Policy Rule - Mobile Users

### Add Security Policy Rule

Best Practice Checks

#### Action and Advanced Inspection

Set the action to take on traffic that matches the criteria you've specified above. By default, this traffic is also scanned for threats based on the best practice security profile settings.

Action \*  
Allow

☐ Send ICMP Unreachable

Profile Group  
Menlo Security Profile

Anti-Spyware

Vulnerability Protection

URL Access Management Menlo-Security

File Blocking

HTTP Header Insertion

WildFire and Antivirus

\* Required Field

Cancel Save

Click Save to accept changes. Then, click Push Config button and Push to apply changes.

Continue with the Common Step 4 and Step 5 further in the document.

## Method 2. Transparent redirection with Prisma Access Traffic Steering

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

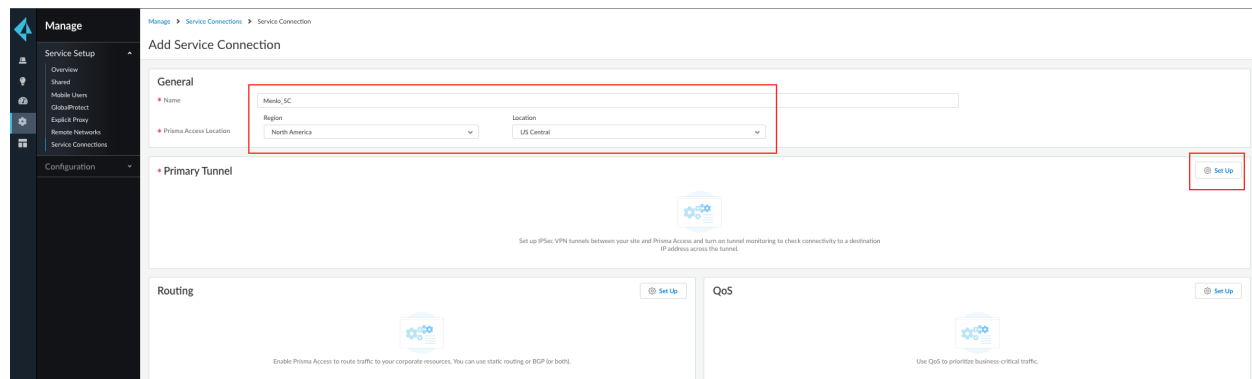
Contact Menlo Security and request the provisioning of an IPSEC tunnel pair.

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

Note - Ensure that the IP address of the Service Connection (available in Step 3) is specified on the tunnel setup on Menlo Security, so that it can accept the connection

Navigate to Manage > Service Setup > Service Connections and create a new Service Connection that will link the Prisma Access instance to the Menlo Security Isolation cloud.



Select a Prisma Access Region and Location as close as possible to 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:

Edit Menlo\_W\_Primary

Back

Tunnel Name \*

Menlo\_W\_Primary

Branch Device Type

Other Devices

Authentication

☒ Pre-Shared Key
☐ Certificate

Pre-Shared Key \*

.....

Confirm Pre-Shared Key \*

.....

IKE Local Identification

FQDN (hostname)
Prisma\_Tunnel\_16\_1

IKE Peer Identification

FQDN (hostname)
Menlo\_16\_Primary

Branch Device IP Address

☒ Static IP
☐ Dynamic

Static IP \*

54.

☐ IKE Passive Mode

☒ Turn on Tunnel Monitoring

Destination IP \*

169.254.10.10

Under the IKE Advanced Options select the following combinations:

#### IKE Advanced Options

[< Back](#)

IKE Protocol Version

IKEv2 only mode

X v

IKEv2 Crypto Profile

Menlo\_Security\_IKE

X v

[Create New](#)

[Manage](#)

☒ IKE NAT Traversal

[Cancel](#)

[Save](#)

#### Edit Menlo\_Security\_IKE

[< Back](#)

Name \*

Menlo\_Security\_IKE

Encryption \*

aes-128-cbc ...

+

Authentication \*

sha256 ...

+

DH Group \*

group19 ...

+

Lifetime

8

Hours

v

IKEv2 Authentication Multiple

0 [<= 50]

\* Required Field

[Cancel](#)

[Save](#)

Under the IPSEC advanced setting, 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 \*

Menlo\_Security\_IPSec

IPSec Protocol

ESP

Encryption \*

aes-128-cbc ...



Authentication \*

sha256 ...



DH Group

group19



Lifetime \*

1

Hours



Lifesize

[1 - 65535]

MB



\* Required Field

Cancel

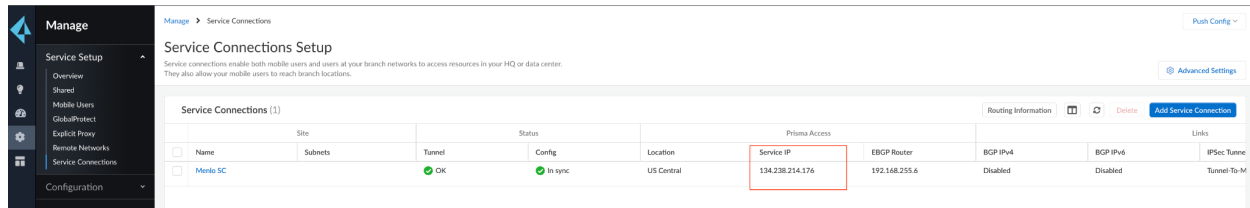
Save

Push the new configuration to accept changes.

Once the Service Connection is created, a dedicated Public IP will get assigned; this will be the IPSEC tunnel endpoint 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.



NOTE: The IP in the picture below is only one random example.



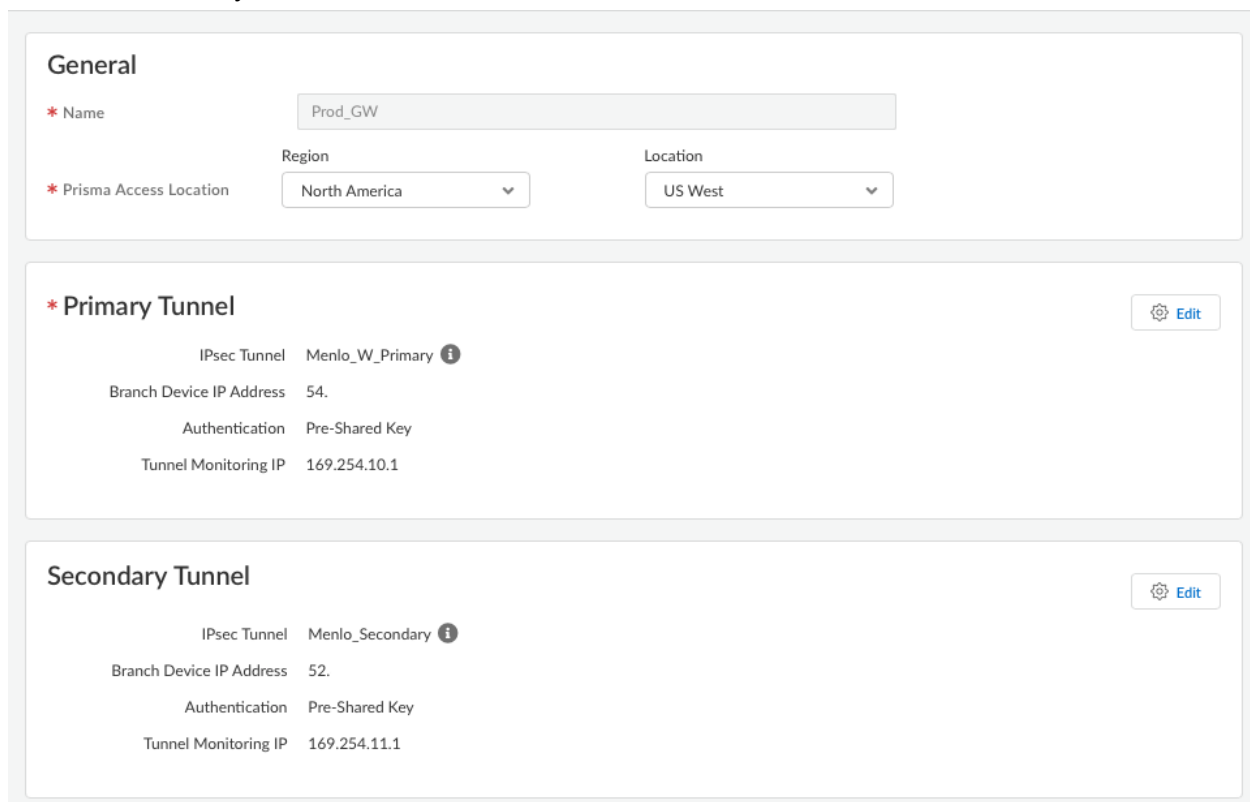
The screenshot shows the 'Service Connections Setup' page in the Menlo Security interface. A table lists service connections, with one entry 'Menlo SC' highlighted. The 'Service IP' for this connection is '134.238.214.176', which is circled in red. Other columns include Name, Site, Tunnel, Status, Config, Location, Prisma Access, EBGIP Router, BGP IPv4, BGP IPv6, and Links.

Name	Site	Tunnel	Status	Config	Location	Prisma Access	EBGIP Router	BGP IPv4	BGP IPv6	Links
Menlo SC			OK	In sync	US Central	134.238.214.176	192.168.255.6	Disabled	Disabled	Tunnel-To-M

Once the IPSEC tunnel is provisioned by Menlo Security as well, validate that the Tunnel status turns into the Green/OK state (please see the picture above)

## 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.



The screenshot shows the configuration page for a service connection. It has two main sections: 'General' and 'Tunnels'.

**General**

- Name: Prod\_GW
- Region: North America
- Location: US West

**Primary Tunnel**

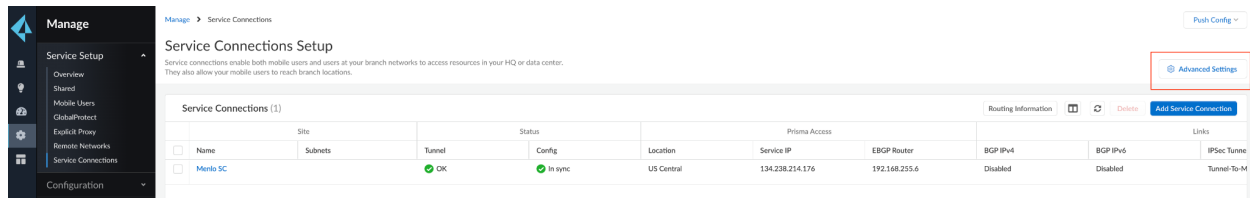
- IPsec Tunnel: Menlo\_W\_Primary
- Branch Device IP Address: 54.
- Authentication: Pre-Shared Key
- Tunnel Monitoring IP: 169.254.10.1

**Secondary Tunnel**

- IPsec Tunnel: Menlo\_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:



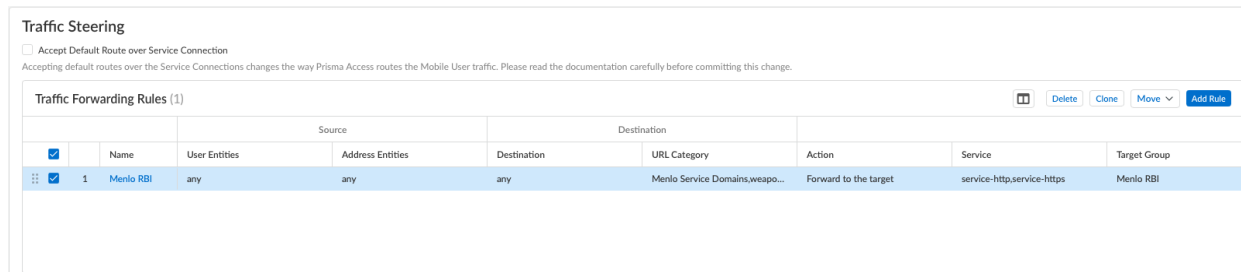
Service Connections Setup

Service connections enable both mobile users and users at your branch networks to access resources in your HQ or data center. They also allow your mobile users to reach branch locations.

Service Connections (1)

Name	Site	Tunnel	Status	Config	Location	Service IP	EBGIP Router	BGP IPv4	BGP IPv6	Links
Menlo SC			OK	In sync	US Central	134.238.214.176	192.168.255.6	Disabled	Disabled	Tunnel-To-M

Under the Traffic Steering menu, create a new Traffic Forwarding rule:



Traffic Steering

☐ Accept Default Route over Service Connection

Accepting default routes over the Service Connections changes the way Prisma Access routes the Mobile User traffic. Please read the documentation carefully before committing this change.

Traffic Forwarding Rules (1)

Name	User Entities	Address Entities	Destination	URL Category	Action	Service	Target Group
1 Menlo RBI	any	any	any	Menlo Service Domains,weapo...	Forward to the target	service-http,service-https	Menlo RBI

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 \*

Menlo RBI

Source

User Entities

Match Any User ▾

Source Address Entities \*

any ▾

Destination

Destination Address Entities

any ▾

URL Category

▾

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 \*

Menlo RBI ▾

Create New Manage

Cancel

Save

## Custom URL Categories

\* Name

Menlo Service Domains

Description

Custom URL Category

\* Type

URL List

Matches any of the following URLs, domains or host names.

Items (1)

Search

Delete

Add

Export

Import

<input type="checkbox"/>	List
<input type="checkbox"/>	*.menlosecurity.com

Enter one entry per row. Each entry may be of the form www.example.com or it could have wildcards like www.\*.com.

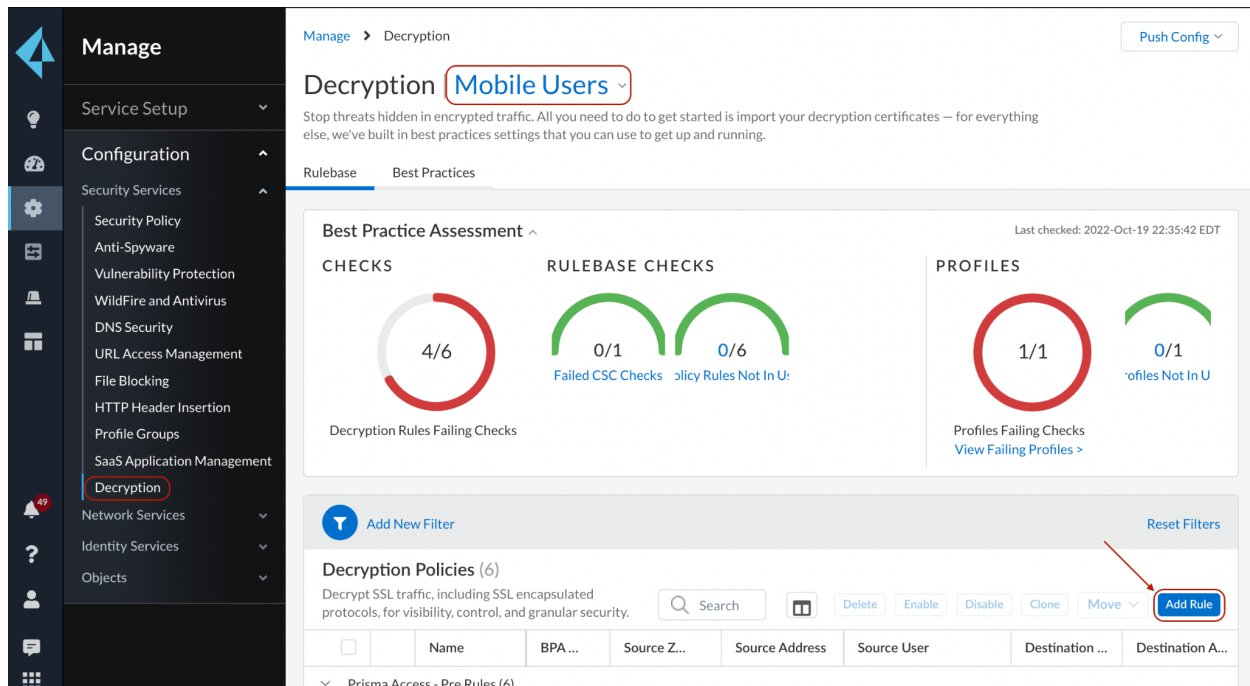
Please note that one of the redirected URL Categories is a custom URL Category that we named “Menlo Service Domains” and contains a wildcard for any URLs under the menlosecurity.com domain.

Push the new configuration to accept changes.

## Common Steps for all integration methods

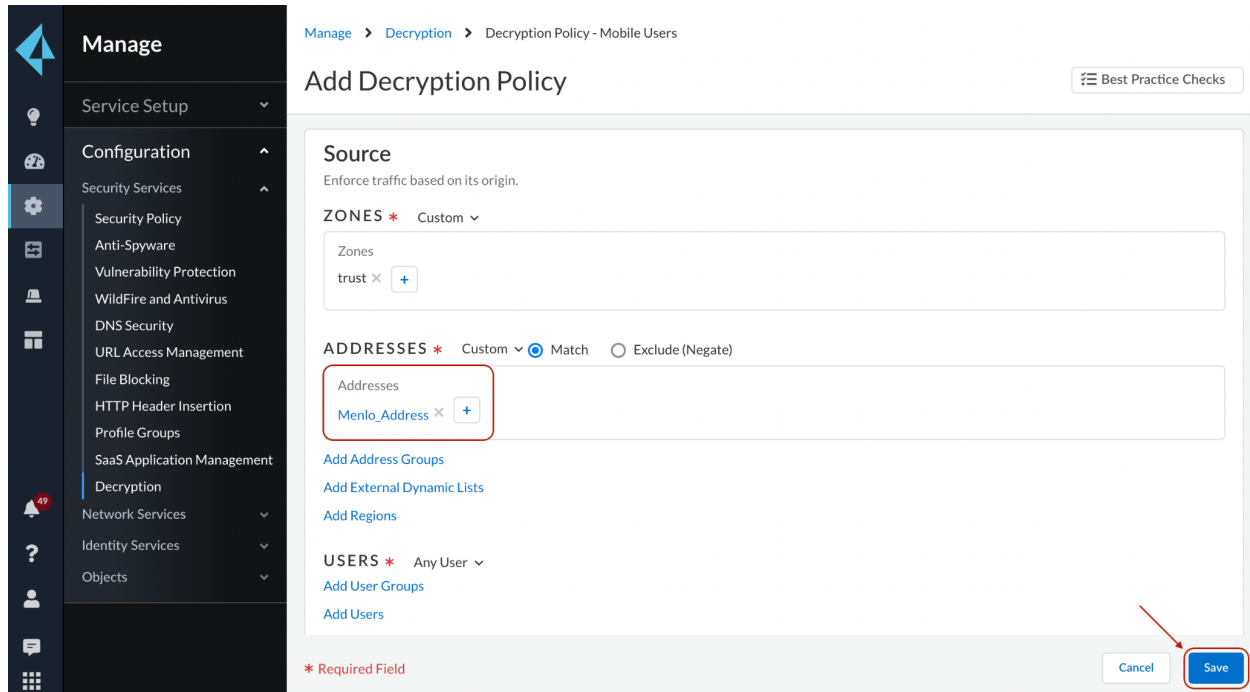
### Step 4: Enable SSL decryption for enhancing the URL Categorization rate

Navigate to Configuration > Security Services > Decryption under the Mobile Users context.  
Create a policy decrypting all the traffic for the required users.



The screenshot shows the Menlo Security management console interface. On the left is a dark sidebar with a 'Manage' section containing 'Service Setup', 'Configuration', and 'Security Services'. Under 'Configuration', 'Decryption' is highlighted. The main content area is titled 'Decryption' with a dropdown menu set to 'Mobile Users'. Below this, there's a 'Best Practice Assessment' section with three circular progress indicators: 'CHECKS' (4/6), 'RULEBASE CHECKS' (0/1 and 0/6), and 'PROFILES' (1/1 and 0/1). Below the assessment is a 'Decryption Policies (6)' section with a table of policies. The table has columns for Name, BPA..., Source Z..., Source Address, Source User, Destination..., and Destination A... The first row is 'Prisma Access - Pre Rules (6)'. A red arrow points to the 'Add Rule' button in the top right of the policies section.

Add the Address object that was created earlier.



Manage > Decryption > Decryption Policy - Mobile Users

### Add Decryption Policy

Best Practice Checks

**Source**  
Enforce traffic based on its origin.

**ZONES \*** Custom ▾

Zones  
trust × +

**ADDRESSES \*** Custom ▾ ☒ Match ☐ Exclude (Negate)

Addresses  
Menlo\_Address × +

[Add Address Groups](#)  
[Add External Dynamic Lists](#)  
[Add Regions](#)

**USERS \*** Any User ▾  
[Add User Groups](#)  
[Add Users](#)

\* Required Field

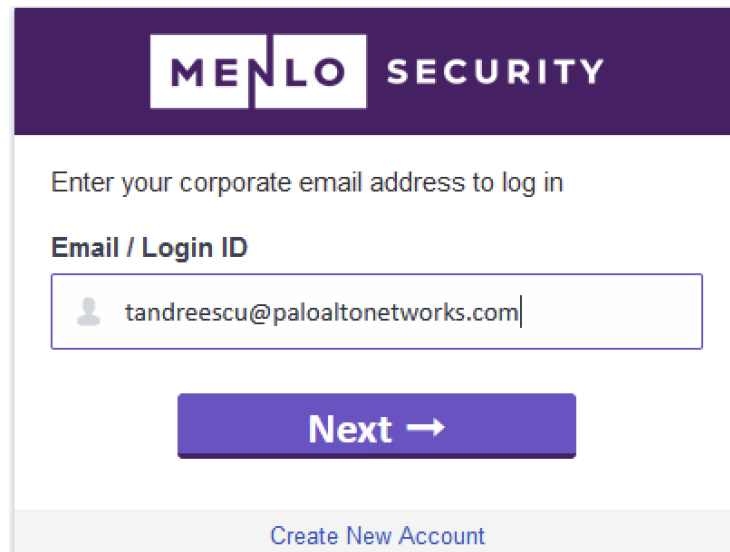
Cancel Save

Push the new configuration to accept changes.

### 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, in our example under the “news” category.

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.

A screenshot of the Menlo Security login interface. At the top is a dark purple header with the "MENLO SECURITY" logo in white. Below the header, the text "Enter your corporate email address to log in" is displayed. Underneath is the label "Email / Login ID" followed by a text input field containing the email address "tandreescu@paloaltonetworks.com". A purple button with the text "Next →" is positioned below the input field. At the bottom of the form, there is a link that says "Create New Account".

*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.*



← → ↺ safe.menlosecurity.com/https://www.bbc.com/


## Welcome to BBC.com



**Pfizer vaccine is '94% effective in over-65s'**


The jab works equally well in people of all ages and ethnicities, further data suggests.

HEALTH



A US city engulfed by Covid but no lockdown

US



The world's biggest scars

FUTURE

## News



### 'No safety concerns' with Pfizer vaccine

Promising new data on the potential



### Trump campaign seeks partial recount in Wisconsin



### BBC vows to 'get to truth' about Diana interview

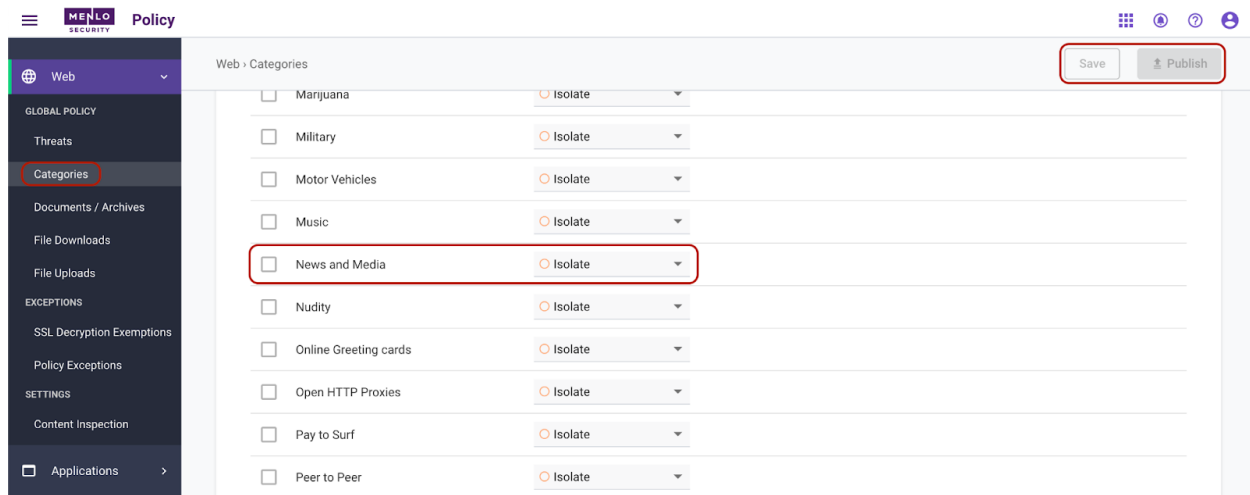
The BBC is investigating allegations



## Menlo Security Configuration

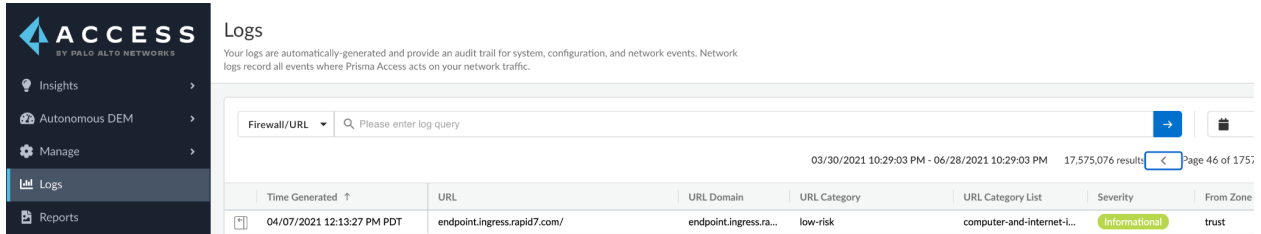
The first two integration methods are using the “prepend” mode in the Menlo Security solution (prepending safe.menlosecurity.com in front of the original URL). This mode will automatically trigger an Isolate action on the Menlo Security so there is no specific configuration required on the Menlo Security 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 Menlo Security > Web Policy > Categories / Threats. This policy ensures that any traffic selected by the Prisma forwarding policy will be isolated by the Menlo Security platform



## 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**  
BY PALO ALTO NETWORKS

Insights  
Autonomous DEM  
Manage  
**Logs**  
Reports

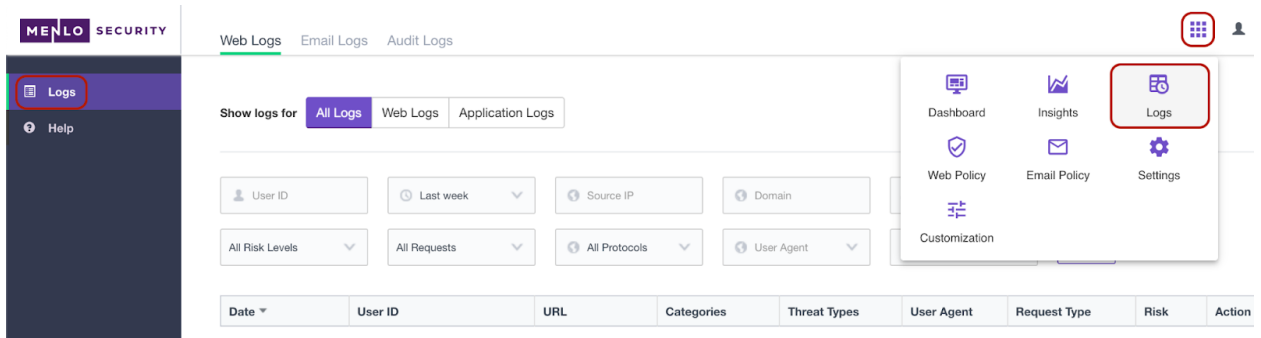
**Logs**  
Your logs are automatically-generated and provide an audit trail for system, configuration, and network events. Network logs record all events where Prisma Access acts on your network traffic.

Firewall/URL 🔍 Please enter log query → 📄

03/30/2021 10:29:03 PM - 06/28/2021 10:29:03 PM 17,575,076 results < Page 46 of 1757

Time Generated ↑	URL	URL Domain	URL Category	URL Category List	Severity	From Zone
04/07/2021 12:13:27 PM PDT	endpoint.ingress.rapid7.com/	endpoint.ingress.ra...	low-risk	computer-and-internet-i...	Informational	trust

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



**MENLO SECURITY**

Web Logs Email Logs Audit Logs

**Logs** Help

Show logs for All Logs Web Logs Application Logs

User ID Last week Source IP Domain  
All Risk Levels All Requests All Protocols User Agent

Dashboard Insights **Logs** Web Policy Email Policy Settings Customization

Date ▼	User ID	URL	Categories	Threat Types	User Agent	Request Type	Risk	Action
--------	---------	-----	------------	--------------	------------	--------------	------	--------