



Technology Partner Program Integration Guide

Author: Menlo Security



Revision History

July 5th, 2021	Validated between Prisma Access and Menlo Security Remote Browser Isolation
----------------	---

Partner Information

Date	July 5th, 2021
Partner Name	Menlo Security
Website	https://www.menlosecurity.com/
Product Name	Menlo Security Isolation Core™
Partner Contact	Head of Strategic Alliances, Sanjit Shah, sanjit.shah@menlosecurity.com
Support Contact	support@menlosecurity.com, 1-866-422-4399
Product Description	Menlo Security Isolation Core™ assumes that all web content is risky and hosts potentially malicious content. This approach eliminates the need to make an “allow or block” determination based on coarse categorization and detailed analysis. Instead, the platform offers an additional option to “isolate” potentially risky or uncategorized websites. For content that is isolated, Menlo efficiently delivers only safe and malware-free content to the end user’s browser with no impact on user experience or productivity, and without requiring an endpoint agent or browser plugins. All active content, such as JavaScript and Flash, whether good or bad, is fully executed and contained within the Menlo Security Isolation Core™. This eliminates the possibility of malware ever leaving the isolated web browsing session within the Isolation Core.

Palo Alto Networks Products for Integration

Table 1: Integration Details by Product

Palo Alto Networks Product	Integration Status	Palo Alto Networks Versions Tested
AutoFocus		
Cortex XDR Prevent		
Cortex XDR Pro		
Next-Generation Firewall		
Panorama		
Prisma Access	Validated	Prisma Access 2.0, 2.1
Prisma Cloud Compute		
Prisma Cloud Enterprise		
Prisma SaaS		

VM-Series		
WildFire		
Other		

Use Cases for Integration with the Palo Alto Security Operating Platform

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 Core™ 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 Core. 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 Core™ via the integration with Prisma Access. This ensures that any website the specified user or group accesses is executed within the cloud-based Menlo Security Isolation Core, 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 via URL prepend, wherein URLs associated with a user’s web traffic are prepended with `safe.menlosecurity.com`.

Integration Benefits

Palo Alto Prisma Access and the Menlo Security Isolation Core™ 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 traffic defined by the use-case criteria (certain users, certain URLs or any combination of both) is redirected to the Menlo Security solution and introduces the air-gap offered by the web-isolation:

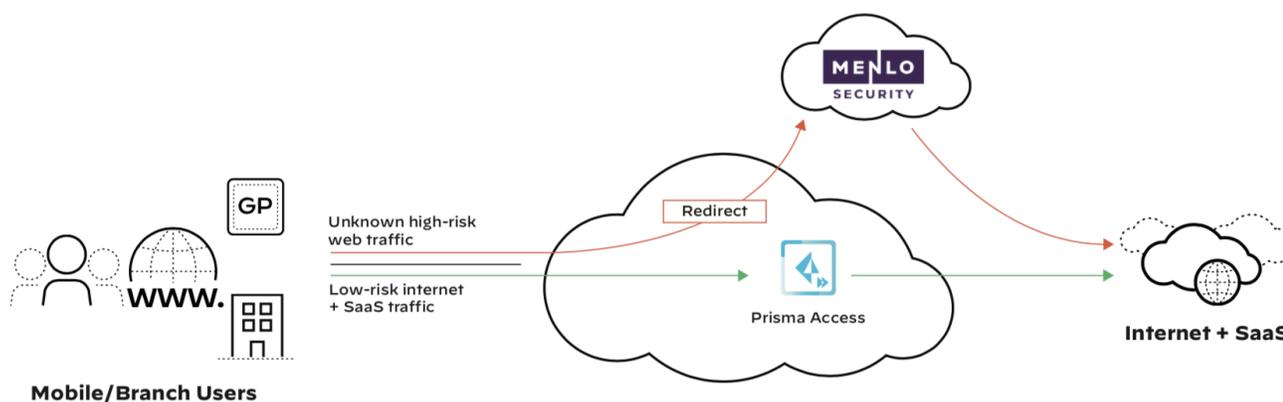


Figure 1: Forwarding of specific traffic to Menlo Security for browser isolation

Before You Begin

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

- Access to the Prisma Access Management platform (Cloud Management or Panorama - the configuration steps are similar)
- Access to a Menlo Security instance and the Admin Portal (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:

- by a “block” “ action set to the desired URL Category and a custom Block Response Page.
- by an “override” action set to the desired URL Category, that can later on be applied to a Security Policy for a specific set of users; this integration method is not supported for the Explicit Proxy Mobile Users.

The configuration details are covered below:

A) 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. 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)

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:

The screenshot shows the Palo Alto Networks Prisma Access Cloud Management portal. The left sidebar is titled 'Manage' and includes sections for Service Setup, Configuration, Security Services, Network Services, Identity Services, and Objects. The 'Configuration' section is expanded to show 'URL Access Management'. The main content area is titled 'test-block URL' and shows the configuration for a URL Access Management Profile for GlobalProtect. The 'Access Control' section is visible, showing a table of URL categories and their Site Access settings. The 'news' category is selected, and the 'Site Access' dropdown menu is open, showing options: Alert, Allow, Block, Continue, and Override. The 'Block' option is highlighted.

Manage > URL Access Management > URL Access Management Profile for GlobalProtect

test-block URL

Configuration Profile Usage

* Name
test-block URL

Security Rules Using This Profile 1
Profile Groups Containing This Profile 1

Access Control

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

Search Category [Set Access] [Set Submission]

<input type="checkbox"/>	Category	Site Access	User Credential Submission	Hits
<input type="checkbox"/>	motor-vehicles	allow	allow	--
<input type="checkbox"/>	music	allow	allow	--
<input type="checkbox"/>	newly-registered-domain	allow	allow	--
<input type="checkbox"/>	news	Block	block	32
<input type="checkbox"/>	not-resolved	allow	allow	--
<input type="checkbox"/>	nudity	allow	allow	--
<input type="checkbox"/>	online-storage-and-backup	allow	allow	--
<input type="checkbox"/>	parked	allow	allow	--
<input type="checkbox"/>	peer-to-peer	allow	allow	--
<input type="checkbox"/>	personal-sites-and-blogs	allow	allow	--
<input type="checkbox"/>	philosophy-and-political-	allow	allow	--

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

Custom Block Response page example:

```
<HTML><HEAD>
<script>

function checkCategory(category, requestedUrl, userID) {
    if (bol_debug) console.log("checkCategory");
    var destination = "https://safe.menlosecurity.com/"+requestedUrl;
    window.location.href = destination;
    console.log("Destination = " + destination);
    //if( 0 <= listCategories.indexOf(category) ){
    //    if (bol_debug) console.log("checkCategory, in if");
    //    If true, the request is blocked and the custom block page shows, if false then the URL is
    redirected to RBI.
    //    var destination = "https://safe.menlosecurity.com/"+requestedUrl;
    //    window.location.href = destination;
    //}
}

function GetAndSetVars(){
    if (bol_debug) console.log("Getandset start");
    userID = document.getElementById("username").innerText;
    requestedUrl = document.getElementById("blockedurl").innerText;
    category = document.getElementById("category").innerText;
    if (bol_debug) console.log("userID: " + userID + " requestedUrl: " + requestedUrl + "
category: " + category);
    checkCategory(category, requestedUrl, userID);
    //checkCategory("gambling", "www.aol.com", "192.168.35.1");
}

// function tagReplace() {
//     document.getElementById("username").innerHTML = "<b>drew</b>";
//     document.getElementById("blockedurl").innerHTML = "www.aol.com";
//     document.getElementById("category").innerHTML = "news";
// }
</script>
<TITLE> Web Page Blocked </TITLE>
<style type="text/css">
.style1 {
    font-family: Verdana;
}
.style2 {
    font-family: Verdana;
    font-size: x-small;
}
.style3 {
    font-size: x-small;
}
</style>
<!-- <script src="https://ajax.googleapis.com/ajax/libs/jquery/3.5.1/jquery.min.js"></script> -->
</HEAD>
<BODY>
<BODY BGCOLOR= '#E0E0E0'>

<p>&nbsp;</p>

<table style="width: 711px; height: 269px;" border="0" cellpadding="0" cellspacing="0" align="center">

    <tbody>

        <tr>

            <td style="vertical-align: top; height: 200px; margin-top: auto;">
```

```

<span style="text-align: center; color: #FF0C05; font-family: Verdana;">
  <center style="width: 726px"><font size="5">Alert Alert - Web Page Blocked
    <br><br>
  </font></center>
</span><span class="style1"><span class="style3"><font size ="3">The site <b><url/></b> you
are trying to access is risky!</b>
  </span></span>.<p><b>

<b>Username:</b> <div id="username"><user/></div><br>
<b>URL:</b> <div id="blockedurl"><url/></div> <br>
<b>Category:</b> <div id="category"><category/></div> <br>
  </span>

  </td>
</tr>
</tbody>
</table>

</BODY></HTML>

<script>
bol_debug = true;
if (bol_debug) console.log("Start");
// tagReplace();
setTimeout(GetAndSetVars,100);
</script>

```

Under URL Access Management>Settings, upload the custom Block Response page under the “URL Access Management Block Page”:

Response Pages (5) Configure the web pages that are displayed when certain actions are triggered.		
Response Page	Location	Actions
Anti Phishing Block Page	predefined	Export HTML Template
Anti Phishing Continue Page	predefined	Export HTML Template
URL Access Management Safe Search Block Page	predefined	Export HTML Template
URL Access Management Block Page	Mobile Users	Revert to Inherited Template Export HTML Template
URL Access Management Continue and Override Page	predefined	Export HTML Template

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

B) 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)

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:

Manage > URL Access Management > URL Access Management Profile for Entire Service

Add URL Access Management Profile

Configuration Profile Usage

* Name

Access Control

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

Search Category Set Access Set Submission

<input type="checkbox"/>	Category	Site Access	User Credential Sub...	Hits
<input type="checkbox"/>	low-risk	allow	allow	--
<input type="checkbox"/>	malware	allow	allow	--
<input type="checkbox"/>	military	allow	allow	--
<input type="checkbox"/>	motor-vehicles	allow	allow	--
<input type="checkbox"/>	music	allow	allow	--
<input type="checkbox"/>	newly-registered-domain	allow	allow	--
<input type="checkbox"/>	news	Override	allow	--
<input type="checkbox"/>	not-resolved	Alert	allow	--
<input type="checkbox"/>	nudity	Allow	allow	--
<input type="checkbox"/>	online-storage-and-backup	Block	allow	--
<input type="checkbox"/>	parked	Continue	allow	--
<input type="checkbox"/>	peer-to-peer	Override	allow	--
<input type="checkbox"/>	personal-sites-and-blogs	allow	allow	--
<input type="checkbox"/>	philosophy-and-political	allow	allow	--

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"

Manage > URL Access Management > Settings

URL Access Management for 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

Define how you want URL category lookups and timeouts to work.

URL Admin Overrides (0)

Allow certain people to access blocked URL categories.

Response Pages (5)

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

Response Page	Location	Actions
Anti Phishing Block Page	predefined	Export HTML Template
Anti Phishing Continue Page	predefined	Export HTML Template
URL Access Management Safe Search Block Page	predefined	Export HTML Template
URL Access Management Block Page	predefined	Export HTML Template
URL Access Management Continue and Override Page	predefined	Export HTML Template

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: support.menlosecurity.com

Manage > URL Access Management > URL Admin Overrides for Mobile Users

Add URL Admin Overrides

URL Admin Override Settings

Mode Transparent Redirect

* Address

* Password

* Confirm Password

SSL/TLS Service Profile

* Required Field

Please 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 Profile Groups and select the Mobile Users context.

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

The screenshot displays the 'Add Profile Group' configuration page in the Palo Alto Networks management console. The left sidebar shows the navigation menu with 'Profile Groups' selected. The breadcrumb trail at the top reads 'Manage > Profile Groups > Profile Group for Mobile Users'. The main content area is titled 'Add Profile Group' and includes a 'Configuration' tab. The 'Profile Group' configuration form contains the following fields:

- Name:** Menlo Profile (marked as a required field with a red asterisk)
- Anti-Spyware Profile:** None
- Vulnerability Protection Profile:** None
- URL Access Management Profile:** Menlo-Security (with a close button 'x')
- File Blocking Profile:** Menlo-Security
- HTTP Header Insertion Profile:** best-practice
- WildFire and Antivirus Profile:** reviewed-best-practice
- DNS Security Profile:** reviewed-best-practice-tytest

A red asterisk and the text '* Required Field' are located at the bottom left of the configuration area.

Navigate to Security Policy 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.

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

Under the Actions tab, select the Allow option and under the Profile Group, select the Profile Group defined in the step above.

Manage > Security Policy > Security Policy Rule for Mobile Users

Add Security Policy Rule

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](#)

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 Profile ▾

Anti-Spyware	
Vulnerability Protection	
URL Access Management	Menlo-Security
File Blocking	
HTTP Header Insertion	

Click the Push Config button and Push..

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.
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, 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.

Welcome

Enter your corporate email address to access this content securely

Next →

OR

If you don't have an account, click Direct Access to navigate directly to the website

Direct Access

[Create New Account](#)

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 current integration is 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.

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:

The screenshot shows the Palo Alto Networks Prisma Access interface. On the left is a navigation menu with options: Insights, Autonomous DEM, Manage, Logs (selected), and Reports. The main area is titled 'Logs' and contains a search bar for 'Firewall/URL' logs. Below the search bar, a table displays log entries. The first entry is highlighted:

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-L...	Informational	trust

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

The screenshot shows the Menlo Security interface. On the left is a navigation menu with options: Dashboard, Logs (selected), Insights, Web Policy, Reporting, Settings, Customization, and Help. The main area is titled 'Web Logs' and contains a search bar for 'All Logs'. Below the search bar, a table displays log entries. The first entry is highlighted:

Date	User ID	URL	Categories ^	Threat Types	Use...	Reques...	R	Action
Jan-08-2021 02:16:09 PM	tandreescu@paloalt...	https://www.fia...	Motor Vehicles		Chrome...	Page Request	LOW	Isolate

On the right side of the interface, there is a sidebar with various details for the selected log entry, including: Web Risk Score (Low), Action (Isolate), User Agent (Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.88 Safari/537.36), Browser Type (Chrome 87), Browser Version, UA Type (Supported Browser), Request Type (Page Request), Request Method (GET), Egress IP (18.209.99.246), and Destination IP (23.222.12.122).

Technical Support

- Contact information for Palo Alto technical support: <https://support.paloaltonetworks.com/>
- Contact information for Menlo Security technical support: support@menlosecurity.com