Technology Partner Program Integration Guide

Author: Menlo Security

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:

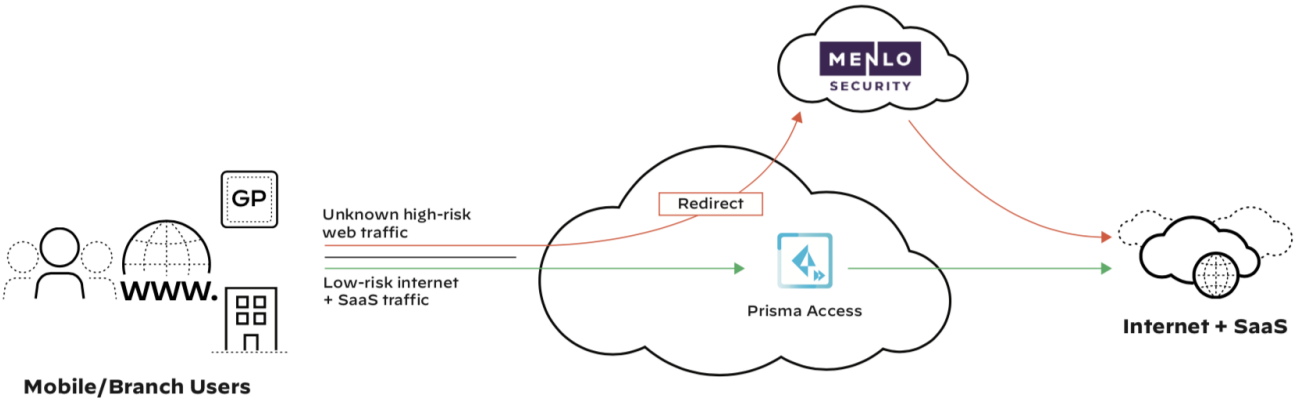


Figure 1: Forwarding of specific traffic to Menlo Security for browser isolation

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:

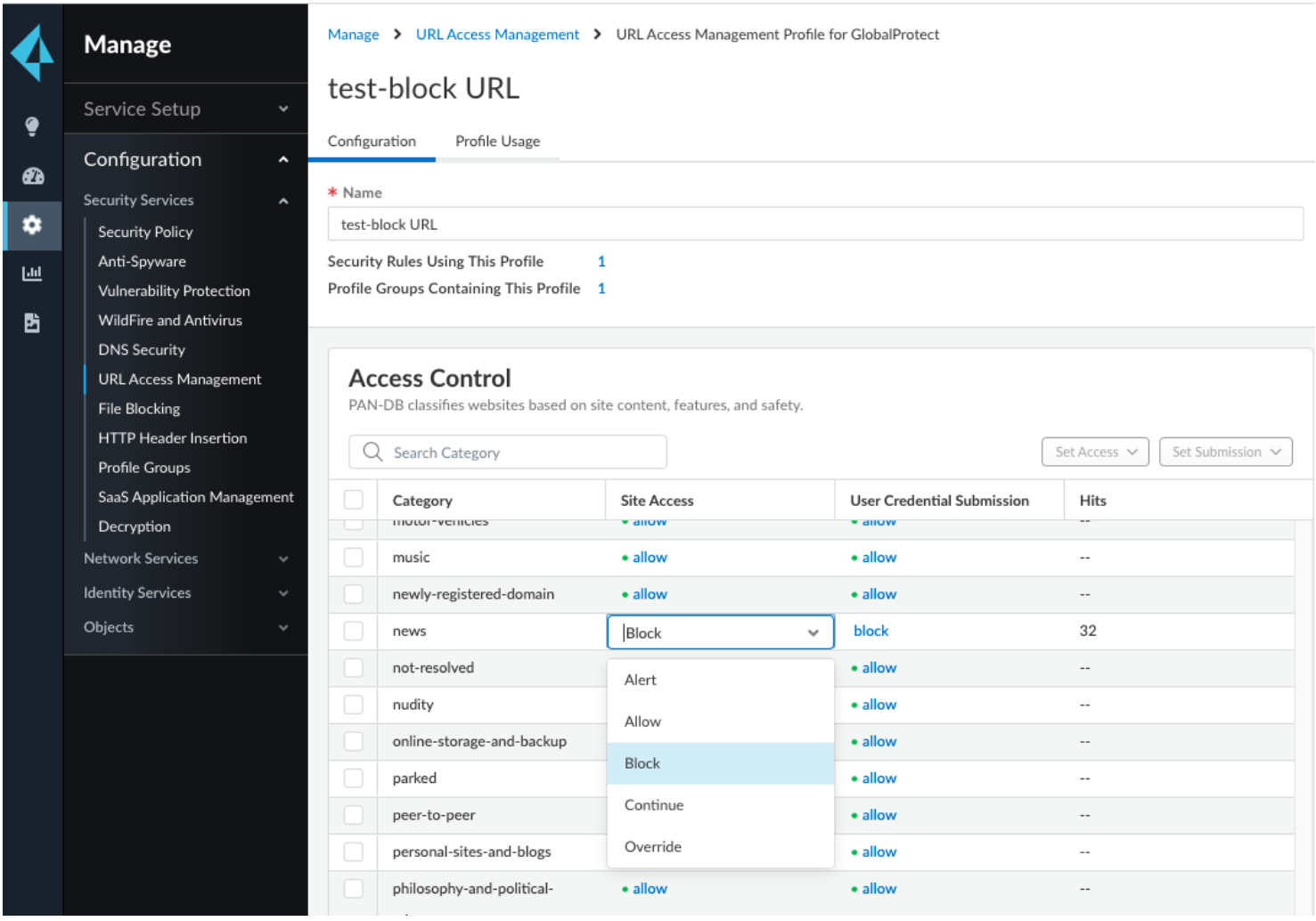
- by a “block” “ action set to the desired URL Category and a custom Block Response Page.
- by an “override” action set to the desired URL Category, that can later on be applied to a Security Policy for a specific set of users; this integration method is not supported for the Explicit Proxy Mobile Users.

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:



Step 2: Upload a custom Block Response Page

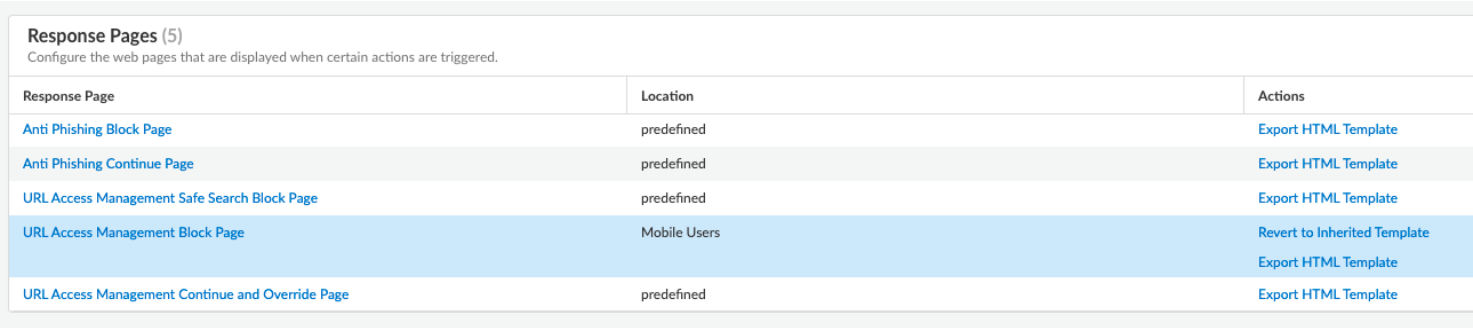
The custom Block Response Page has the role of prepending “safe.menlosecurity.com” in front of the original URL requested by the user, once that URL matches the URL Category we want to send through isolation.
An example of a Block Response age is listed below but this can be changed and adapted for more 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> </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":

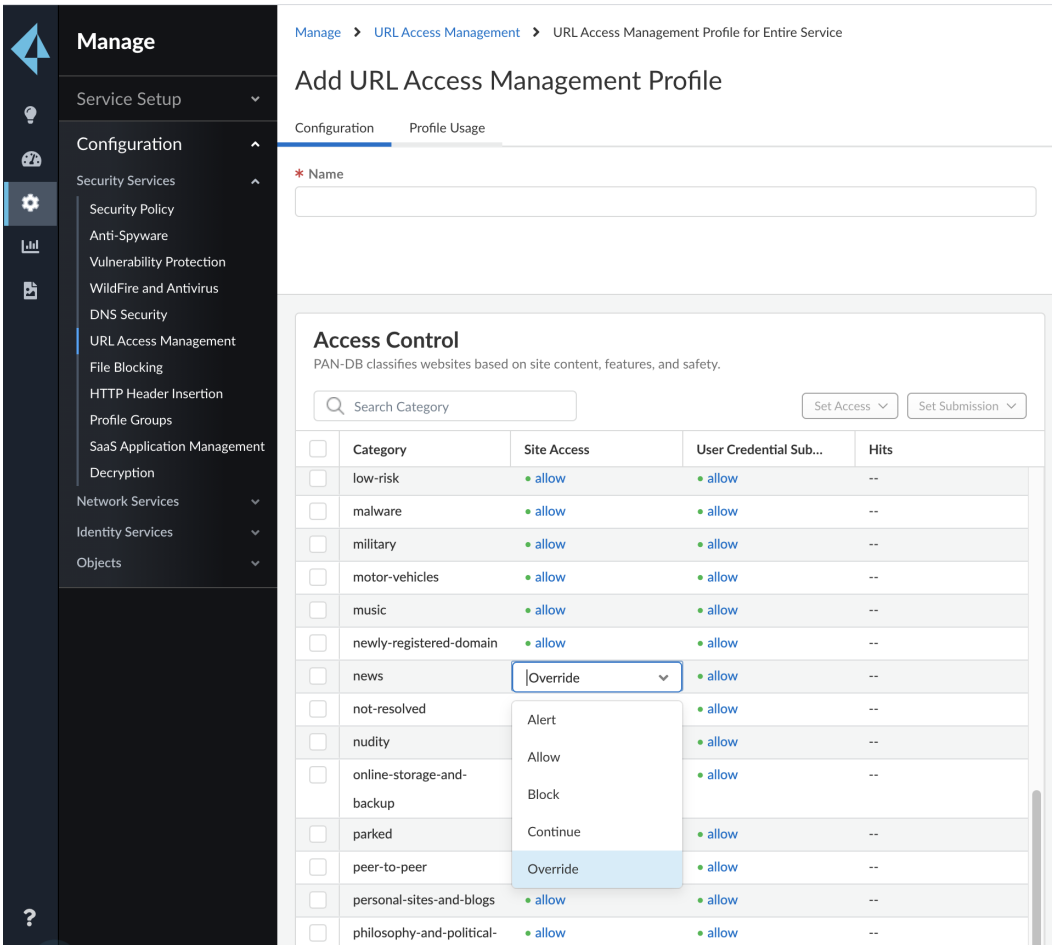


Please continue with Step 3 as the configuration is similar for both methods from that point on.

B) Override action Integration method

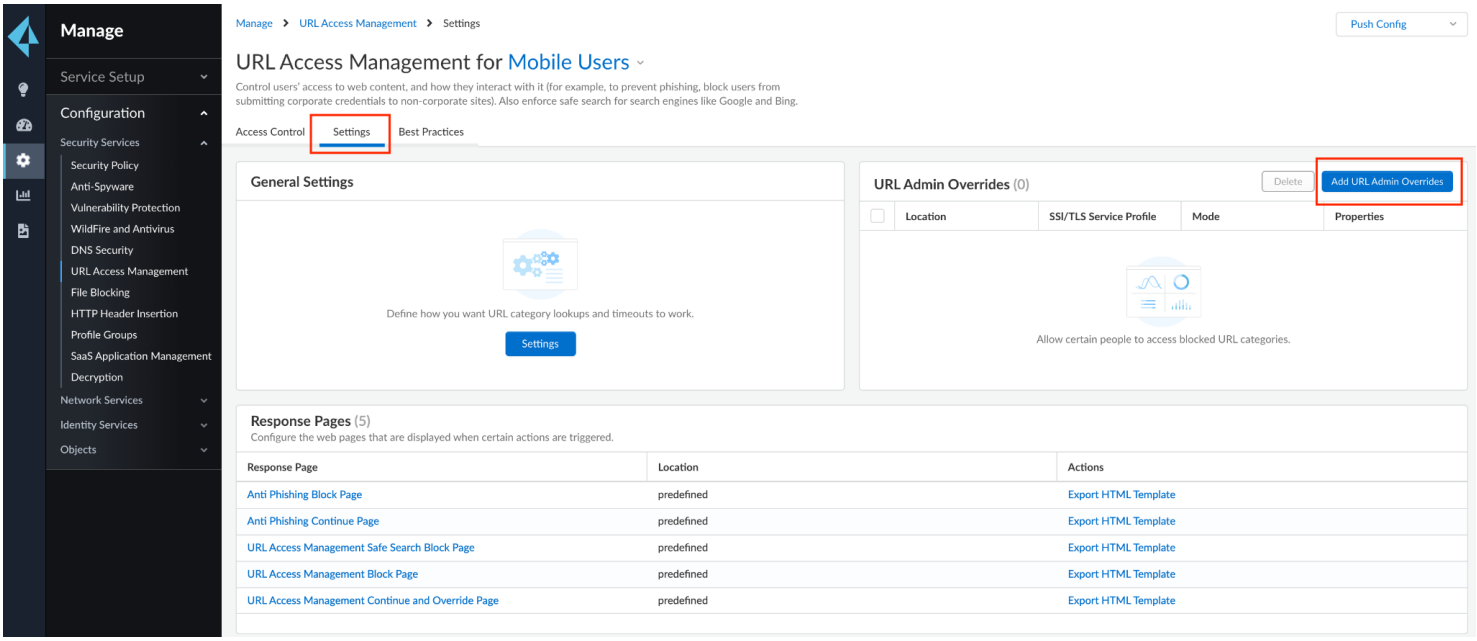
Step 1: Set the desired URL Filtering Category to Override

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:



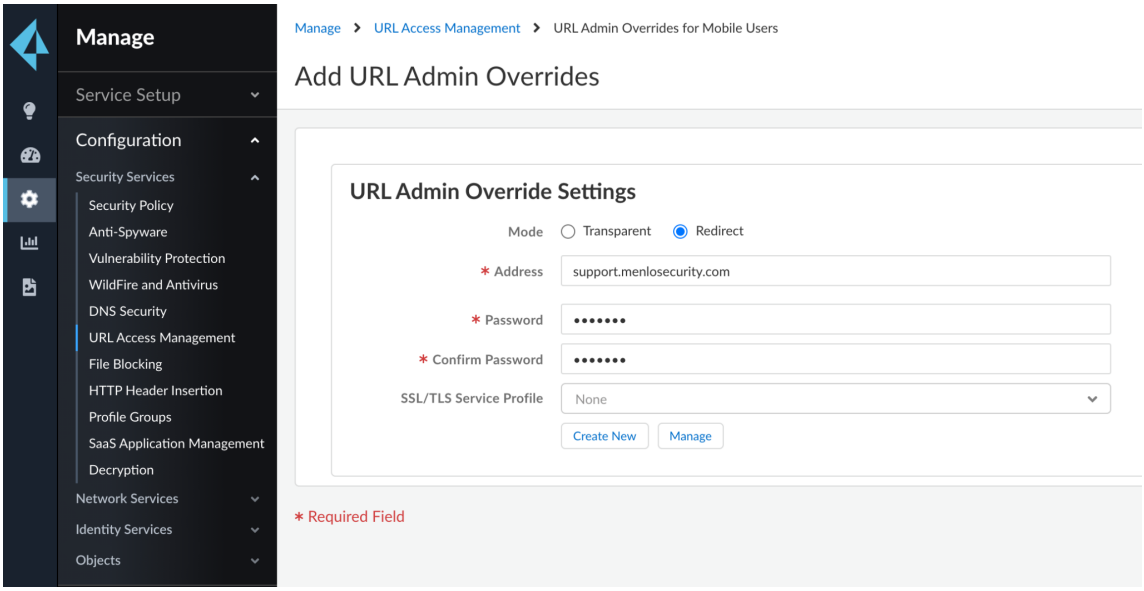
Step 2: Set the destination address to be used for the Override action

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

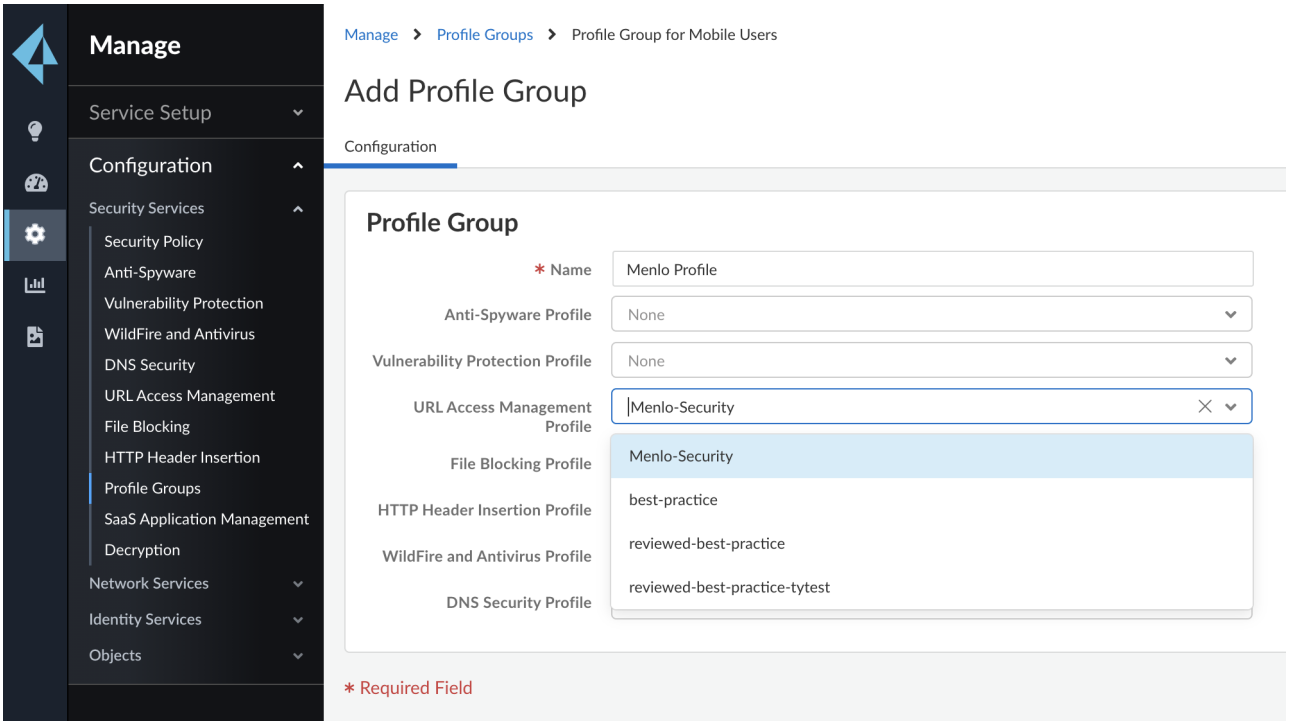
- Password and Confirm Password: Any password: this is the password that you share with your users who are allowed the override privilege. This is not used in the Menlo Security integration.
- SSL/TLS Service Profile: None
- Mode: Redirect
- Address: support.menlosecurity.com



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

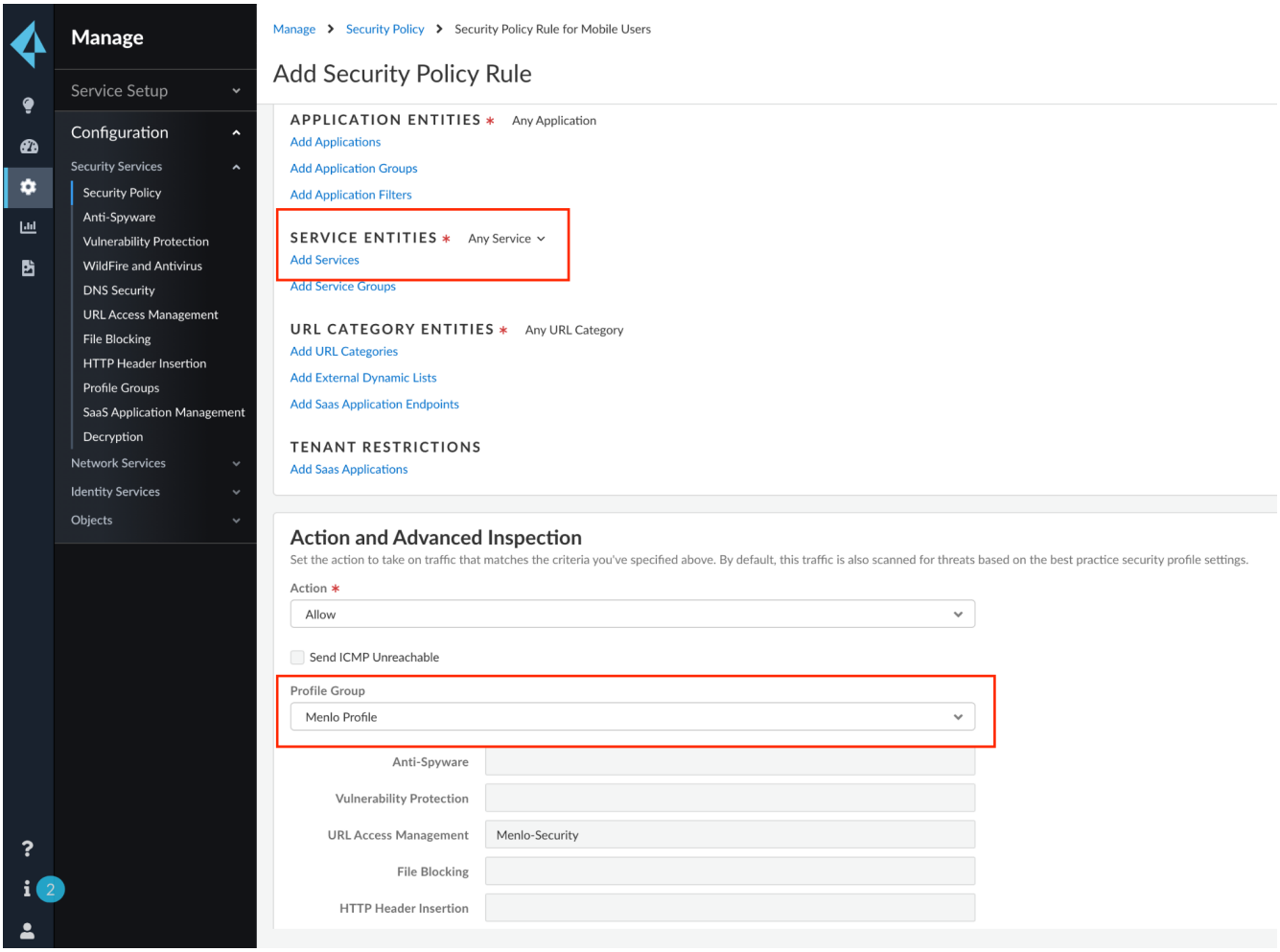
Step 3: Update the policy handling the Internet bound traffic with the previously created URL Access Management profile

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.



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.



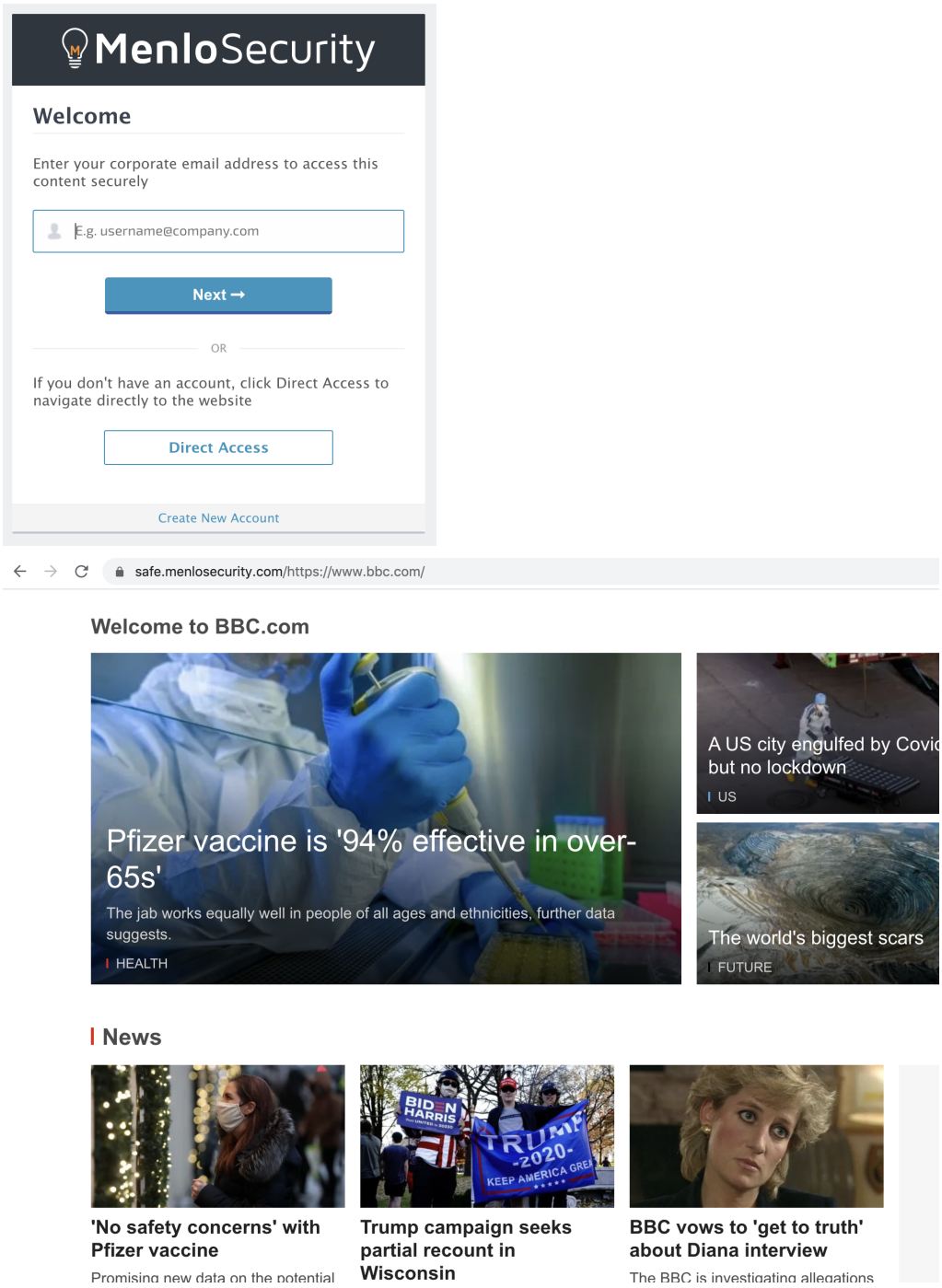
Click the Push Config button and Push..

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.

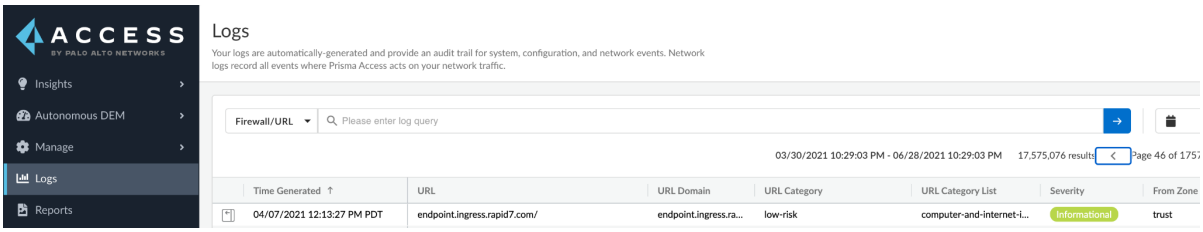


Menlo Security Configuration

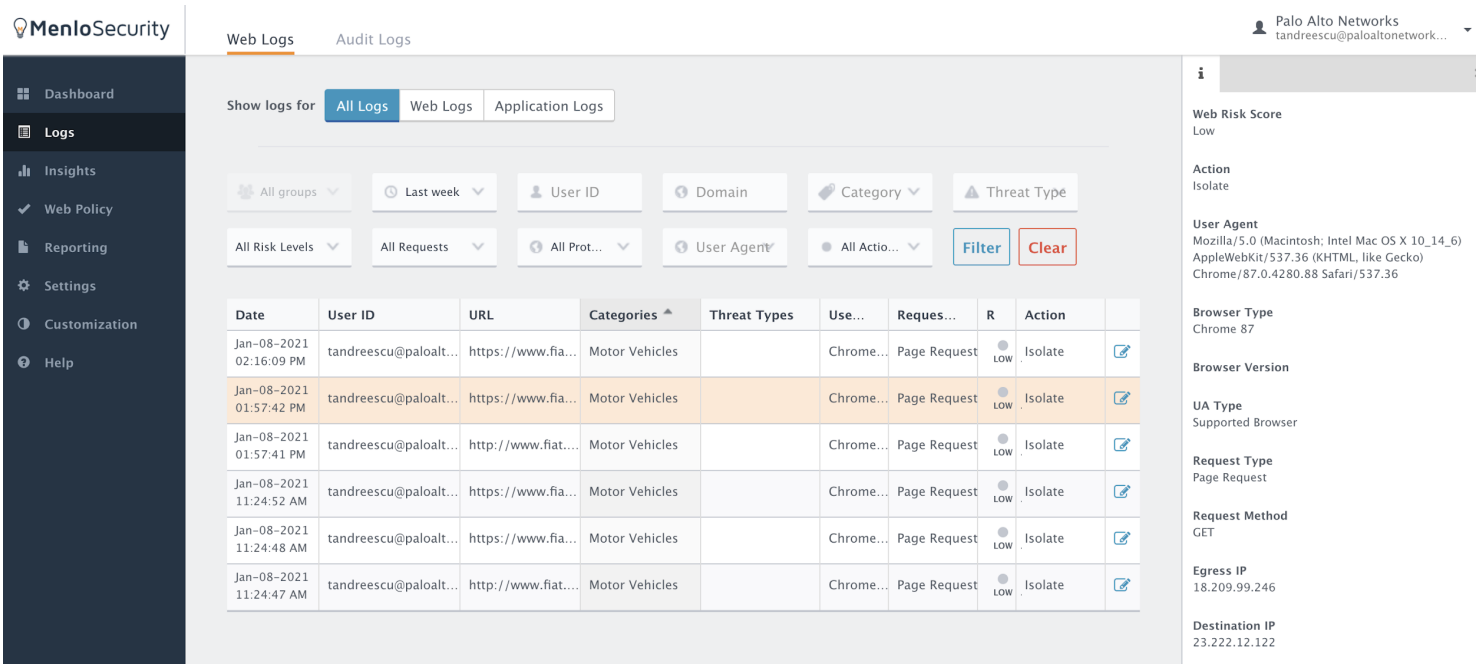
The current integration is using the “prepend” mode in the Menlo Security solution (prepending safe.menlosecurity.com in front of the original URL). This mode will automatically trigger an Isolate action on the Menlo Security so there is no specific configuration required on the Menlo Security side.

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



Technical Support

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