

How to set up PacketFence with OPSWAT MetaAccess Client

Contents

About This Guide.....	2
Part 1: Enforce MetaAccess client installation	3
Step 1:	3
Step 2:	3
Step 3:	5
Step 4:	6
Step 5:	7
Part 2: Enforce device compliance.....	9
Step 1:	9
Step 2:	11

About This Guide

OPSWAT MetaAccess (formerly Metadefender Endpoint Management) is a cloud based access control solution that helps organizations enforce endpoint compliance and prevent contamination of cloud applications by blocking potentially compromised or non-compliant devices from accessing SaaS applications. More information on MetaAccess can be found at <https://www.opswat.com/cloud-access-control>

MetaAccess can be leveraged by PacketFence network access control policies to provide enhanced compliance checking capabilities for this Open Source NAC solution. This guide specifically illustrates how to establish MetaAccess policy checks by creating a provisioner in PacketFence to enforce installation of the MetaAccess client on devices as well as to check for device compliance before and during network access. Standard PacketFence configuration options are outside the scope of this guide.

More information on the benefits of integrating MetaAccess with PacketFence can be found at <https://www.opswatMetaAccess.com/integration/secure-access>.

Part 1: Enforce MetaAccess client installation

The following steps will walk you through gathering the information needed and creating the OPSWAT MetaAccess provisioner in PacketFence in order to ensure that each device registering with or attempting to access your network has the MetaAccess client installed.

Step 1:

Using your OPSWAT MetaAccess account, log in to the MetaAccess Developer Portal at <https://MetaAccess.opswat.com/developers>. Register a new application, making sure to set the callback URL to <http://127.0.0.1/opswat>. Make a note of the client key and client secret for use in later steps.

OAuth Settings

Client key	024P5ABG4QAC0F0H0123040Y798K7H8279KLU8
Client secret	8QJ0B0W45794048K50P020279PL0HEM0HG879AS00E
Callback URL	http://127.0.0.1/opswat

Step 2:

Generate an OAuth2 access and refresh tokens to enable PacketFence to access the OPSWAT MetaAccess cloud API.

First, go to the following URL in your browser, replacing **-clientkey-** with the client key you obtained in the previous step:

https://MetaAccess.opswat.com/o/oauth/authorize?client_id=-clientkey- &response_type=code&redirect_uri=http://127.0.0.1/opswat

Click the button to authorize this application:

ACCESS AUTHORIZATION

Authorize PacketFence test to have read access your protected resources.



You will be redirected to an unavailable page, but the URL will contain your authorization code in its parameters.

Example:

<http://127.0.0.1/opswat?code=hL8wsl>

Use this code to generate the access and refresh token through another HTTP request in your browser. Go to the following URL in your browser, replacing `-clientkey-` and `-clientsecret-` with the values you obtained in step 1, and replacing `-authcode-` with the code you obtained just above:

https://MetaAccess.opswat.com/o/oauth/token?client_id=-clientkey-&client_secret=-clientsecret-&grant_type=authorization_code&redirect_uri=http://127.0.0.1/opswat&code=-authcode-

You should now be presented with a JSON response that contains the access and refresh tokens. Take note of these values for the PacketFence configuration. Example:

```
{ "access_token": "75c320e8-8bdd-4ac4-9406-93d9d9fff624", "token_type": "bearer", "refresh_token": "27479745-f50d-4d84-ad70-f289e3e5f94a", "expires_in": 43199, "scope": "read", "client_id": "CX5MYSIABG4QAICRFOHD123SXJM2VI7BNBCY4H9Z1WNKUIY8" }
```

Step 3:

Now you will create a new provisioner in PacketFence. Log into the PacketFence administration interface, then go to the *Configuration* tab and go to *Provisioners*. Click *Add provisioner* and select *opswat*.

Configure this provisioner using the information obtained in steps 1 and 2.

The screenshot shows the PacketFence Provisioning interface. On the left, there is a sidebar with a list of provisioners: android, ios, mobileron, and opswat. Below the list is a button labeled 'Add provisioner'. The main area displays a 'New Provisioning Entry' form with the following fields:

Provisioning ID	opswat
Description	OPSWAT
Set role	Select a role
Client Id	1234567890
Client Secret	0987654321
Host	gears.opswat.com
Port	443
Protocol	https
Access token	b5275f8c-a22c-4260-8090-696c2b3
Refresh token	ec532cc4-0d78-426e-8c44-1411c5t
Agent download uri	https://gears.opswat.com/gears/a/dc

At the bottom right of the form, there are 'Close' and 'Save' buttons.

The Provisioning ID is the friendly name of the provisioner.

The Client Id is the client key of the application, which you obtained in step 1.

The Client Secret is the secret of the application, which you obtained in step 1.

In most cases the Host will be MetaAccess.opswat.com, unless you are testing against the MetaAccess beta site or an on-premises deployment.

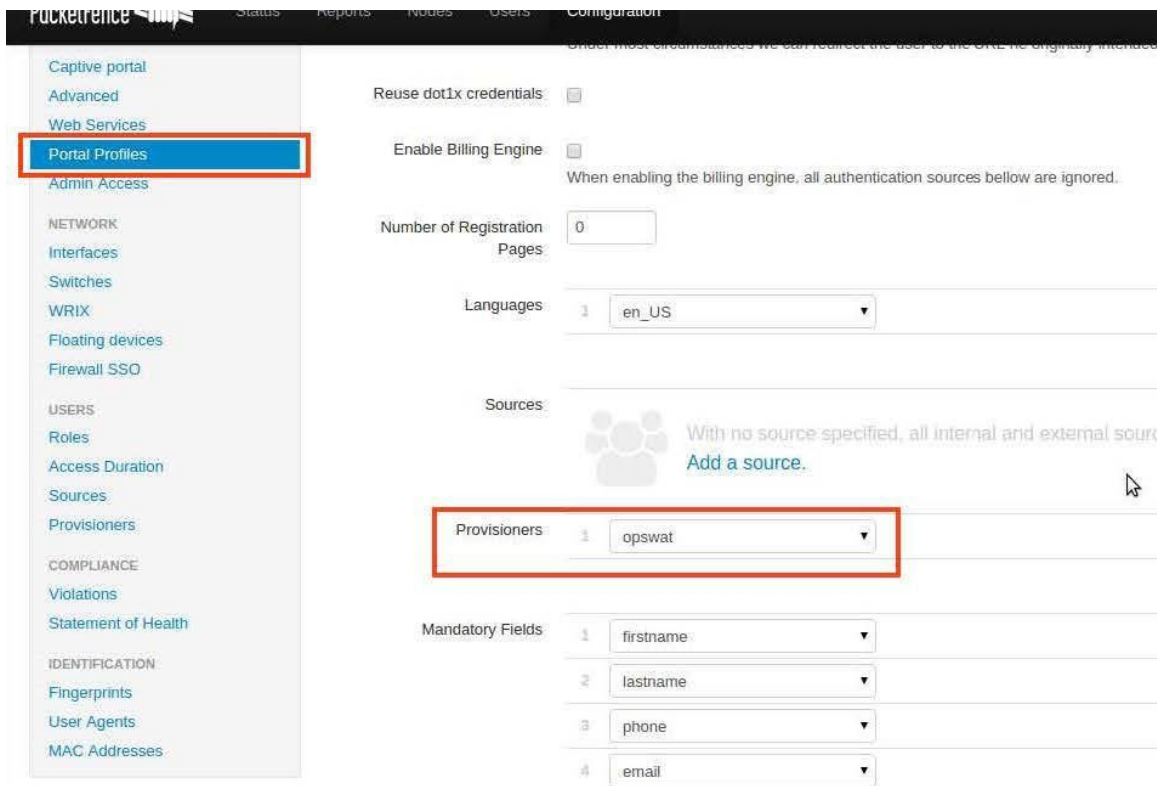
The port and protocol should be left to default.

The access and refresh tokens are the tokens you obtained at the end of step 2.

The Agent download URI is the download URL specific to your MetaAccess account. You can obtain this by logging into your MetaAccess account, clicking +DEVICES, and choosing to *Enable MetaAccess client on this device*. The URL that opens is the account specific download URI you need

Step 4:

Now that you have created the provisioner in PacketFence, go to the *Portal Profiles* menu on the left and select the default portal. Click *Add Provisioner* and select the new OPSWAT MetaAccess provisioner that was created in step 3.

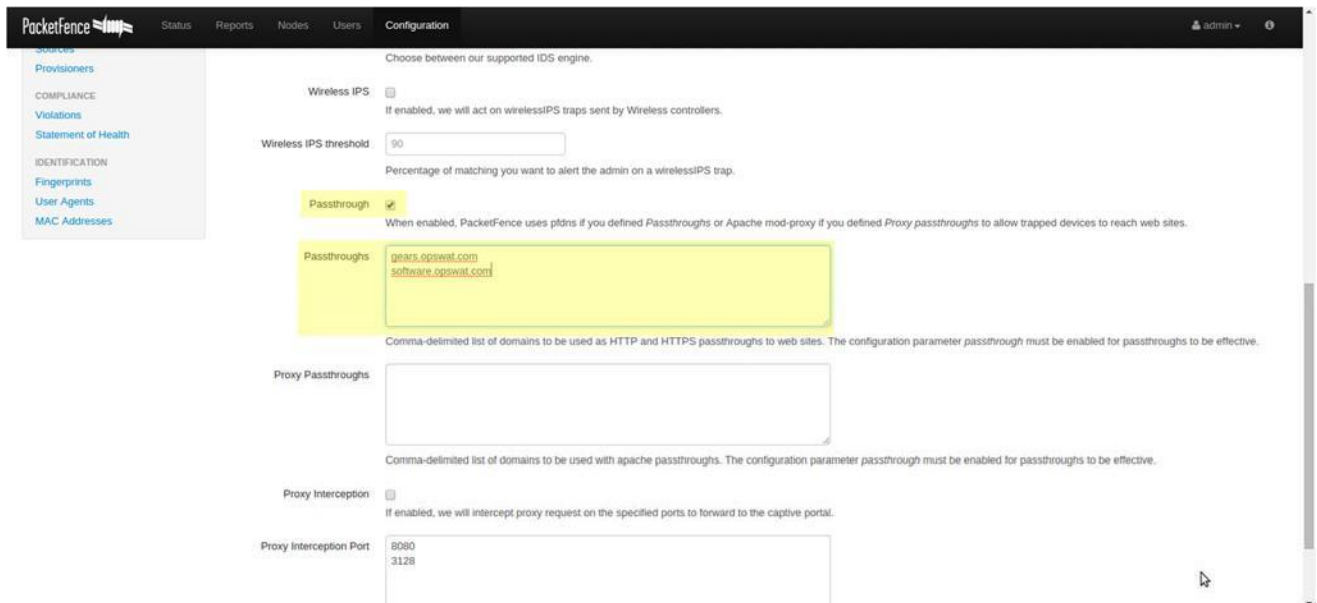


Step 5:

Next, still in the PacketFence administration console, go to *Trapping* in the left menu, then scroll to *Passthroughs*. Check the *Passthrough* box above the field and add the following domains to the passthrough list:

MetaAccess.opswat.com

software.opswat.com

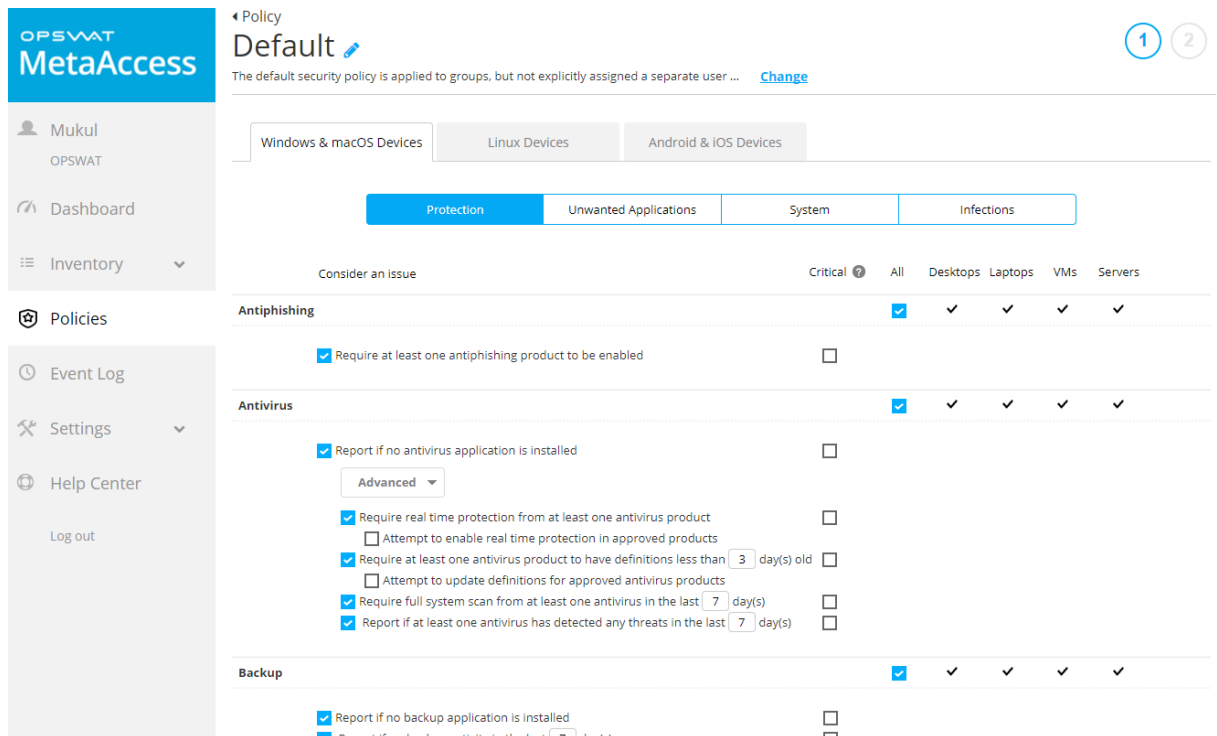


You have now finished configuring PacketFence to enforce installation of the MetaAccess client. You can test this by connecting a device to your test network and registering as you normally would. At the end of the registration process, you will be presented with a page asking you to install the MetaAccess client on your device. After installing, click continue, and if your access is enabled then PacketFence and MetaAccess are correctly connected.

Part 2: Enforce device compliance

In this section, the steps will guide you in configuring PacketFence to enforce device compliance with MetaAccess policies before and during network access.

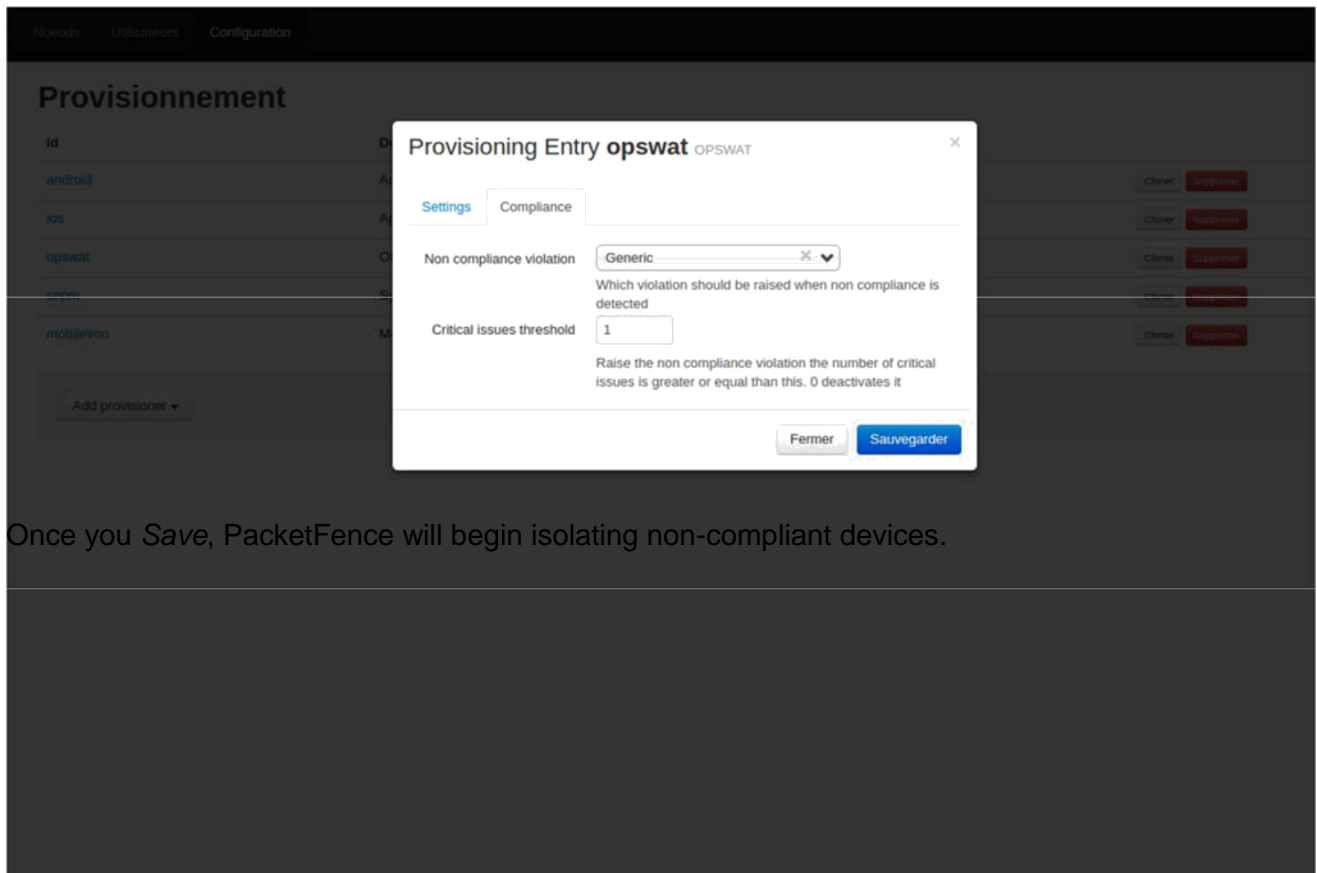
Before configuring PacketFence, configure your device policy in MetaAccess to indicate what you consider an issue or critical issue. PacketFence will utilize the number of critical issues as an access threshold.



Step 1:

Configure the OPSWAT MetaAccess provisioner to activate the enforcement of compliance using your critical issues. In the provisioner configuration, go to the *Compliance* tab. You can select which violation should be raised when a device is non-compliant; *Generic* can be used to get started, and can be adjusted in Step 2. In the *Critical issues threshold* field, enter the

number of critical issues a device needs to have before PacketFence should isolate it. Entering “1” will isolate the device whenever there is at least one critical issue.



The screenshot shows the OPSWAT Provisionnement interface. A modal window titled "Provisioning Entry opswat OPSWAT" is open, displaying the "Compliance" settings. The "Non compliance violation" is set to "Generic", and the "Critical issues threshold" is set to "1". The modal also includes a "Fermer" button and a "Sauvegarder" button.

Provisionnement

Id

android

ios

opswat

macos

mobileiron

Add provisionner

Provisioning Entry opswat OPSWAT

Settings Compliance

Non compliance violation Generic

Which violation should be raised when non compliance is detected

Critical issues threshold 1

Raise the non compliance violation the number of critical issues is greater or equal than this. 0 deactivates it

Fermer Sauvegarder

Once you Save, PacketFence will begin isolating non-compliant devices.

Step 2:

You can now customize the template the violation is using in the *Portal Profile* section. Simply select your portal profile and then go to the *Files* tab. Here you can modify the `violations/generic.html` template so that it displays additional information. You can also customize this violation in the *Violations* section of the administration interface. Refer to the PacketFence Administration Guide for additional information.

PacketFence is now configured to enforce installation of the MetaAccess client as well as device compliance. For more information, or if you have any questions about the steps above, please log into the OPSWAT Portal at <https://myportal.opswat.com> and submit a ticket to request assistance from our support team.