OPSWAT.
MetaAccess

How to set up VMware Unified Access Gateway with OPSWAT MetaAccess Client

About This Guide

OPSWAT MetaAccess (formerly Metadefender Endpoint Management) is a cloud based next generation network access control solution that helps organizations enforce endpoint compliance and prevent contamination of cloud applications by blocking risky devices from accessing SaaS applications. More information on MetaAccess can be found at https://www.opswat.com/products/metaaccess

MetaAccess can be leveraged by VMware Unified Access Gateway (UAG) 3.1 and newer to provide enhanced compliance checking capabilities for Horizon Client access to virtual desktops and RDS hosted applications. This guide specifically illustrates :

1. how to establish MetaAccess policy checks by setting up UAG Endpoint Compliance Check Provider Settings to enforce installation of the MetaAccess client on Horizon client devices and
2. how to check for device compliance before allowing access to virtual desktops or RDS hosted applications.

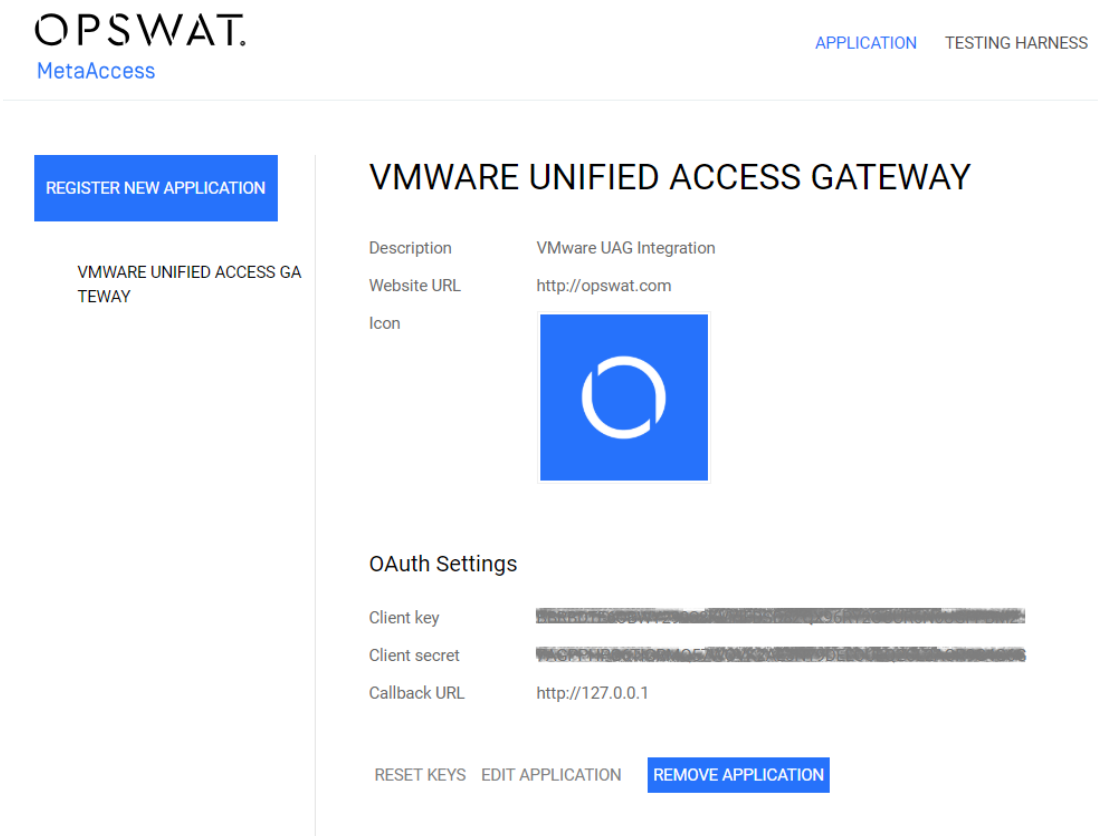
belong to their respective owners.

Part 1: Enforce MetaAccess client installation

The following steps will walk you through gathering the information needed and creating the OPSWAT MetaAccess configuration in VMware UAG Endpoint Compliance Check Provider Settings. This will ensure that each Horizon Client device accessing VMware Horizon desktops and RDS hosts through UAG has the MetaAccess client installed and meets the policy defined in MetaAccess.

Step 1:

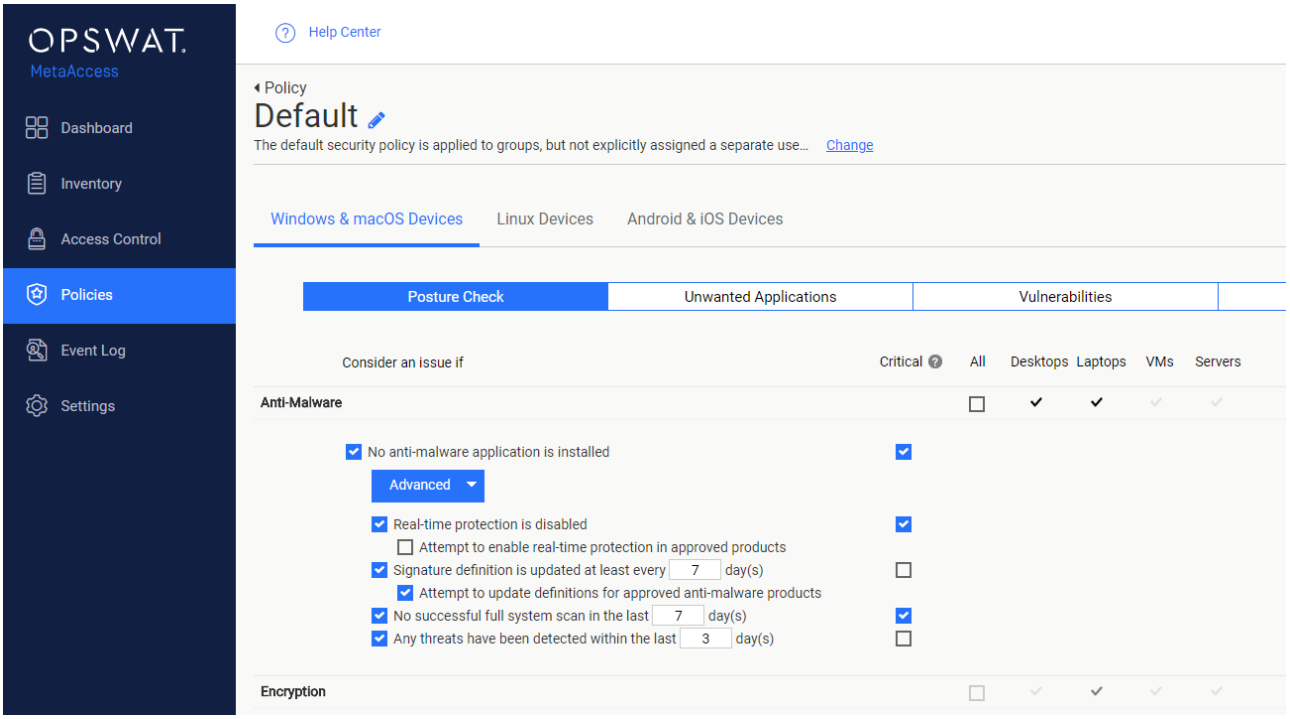
Using your OPSWAT MetaAccess account, log in to the MetaAccess oAuth Portal at https://gears.opswat.com/o. Register a new application, making sure to set the callback URL to http://127.0.0.1/opswat. Make a note of the client key and client secret for use in later steps.



Part 2: Enforce device compliance

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

Before configuring UAG, configure your device policy in MetaAccess to indicate what you consider an issue or critical issue. UAG will deny access from any endpoint that has one or more critical issues.

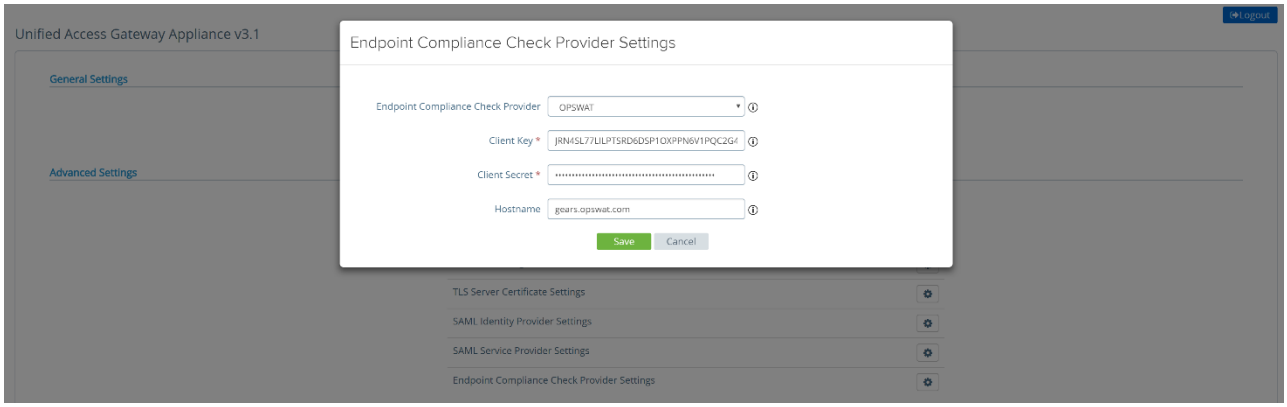


Step 1:

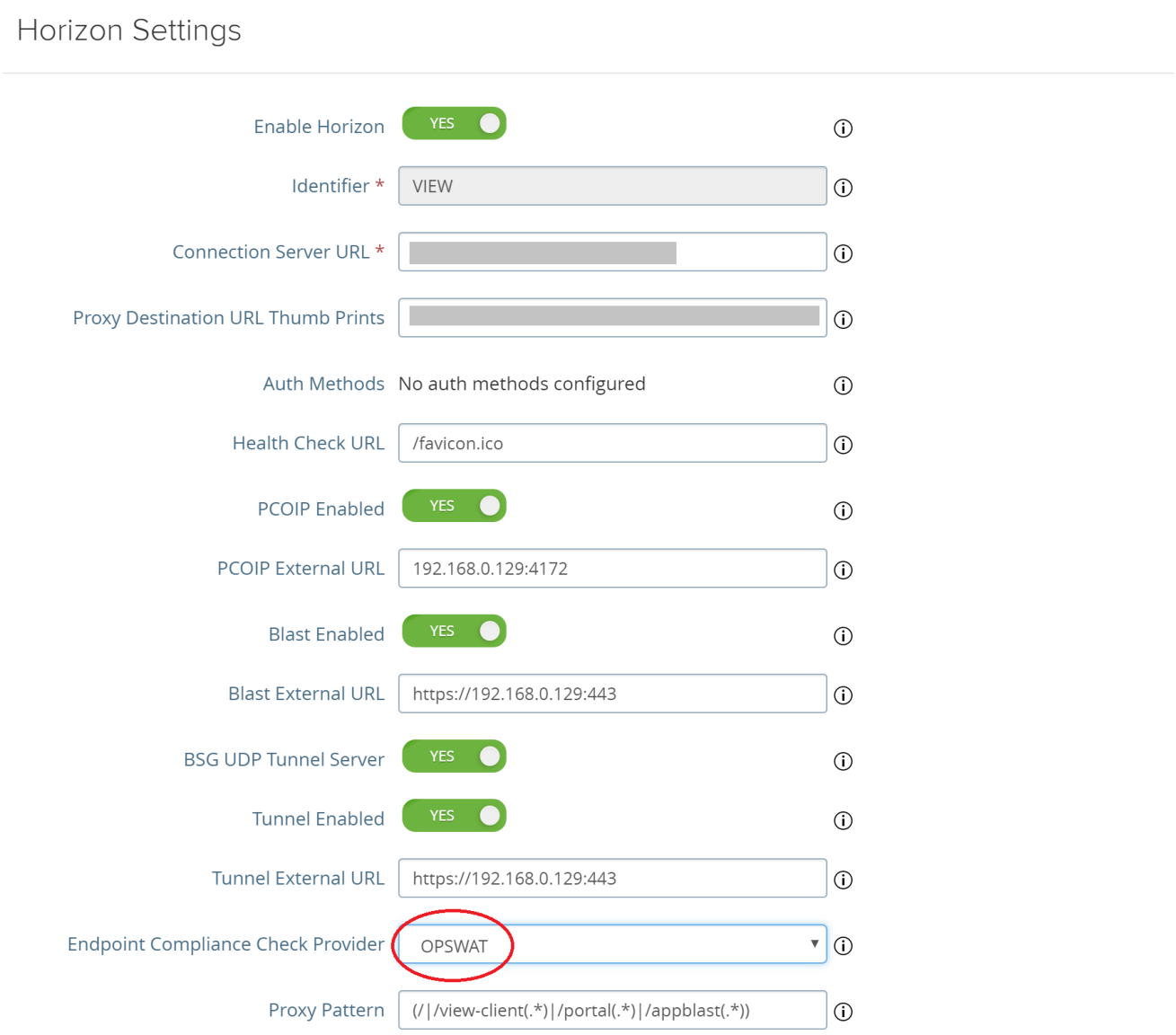
Configure Endpoint Compliance Check Provider Settings in UAG. This can either be done through the UAG Admin GUI or through settings in your PowerShell .ini file for UAG.

From the UAG Admin console in *Advanced Settings*, go to *Endpoint Compliance Check Provider Settings*. Click *Add*. From the *Endpoint Compliance Check Provider* dropdown list, select *OPSWAT*.

Copy and paste the client_id and client_secret values that you obtained in step 1, leave the hostname set to the default of `gears.opswat.com` and click *Save*.



In General Settings select *Show* next to *Edge Service Settings*. Select *Horizon Settings* and then under *More*, go to *Endpoint Compliance Check Provider*.



In the dropdown list select *OPSWAT* and then click *Save*.

UAG is now configured to enforce endpoint compliance for VMware Horizon client access. For more information, or if you have any questions about the steps above, please log into the OPSWAT Portal at https://portal.opswat.com and submit a ticket to request assistance from our support team.