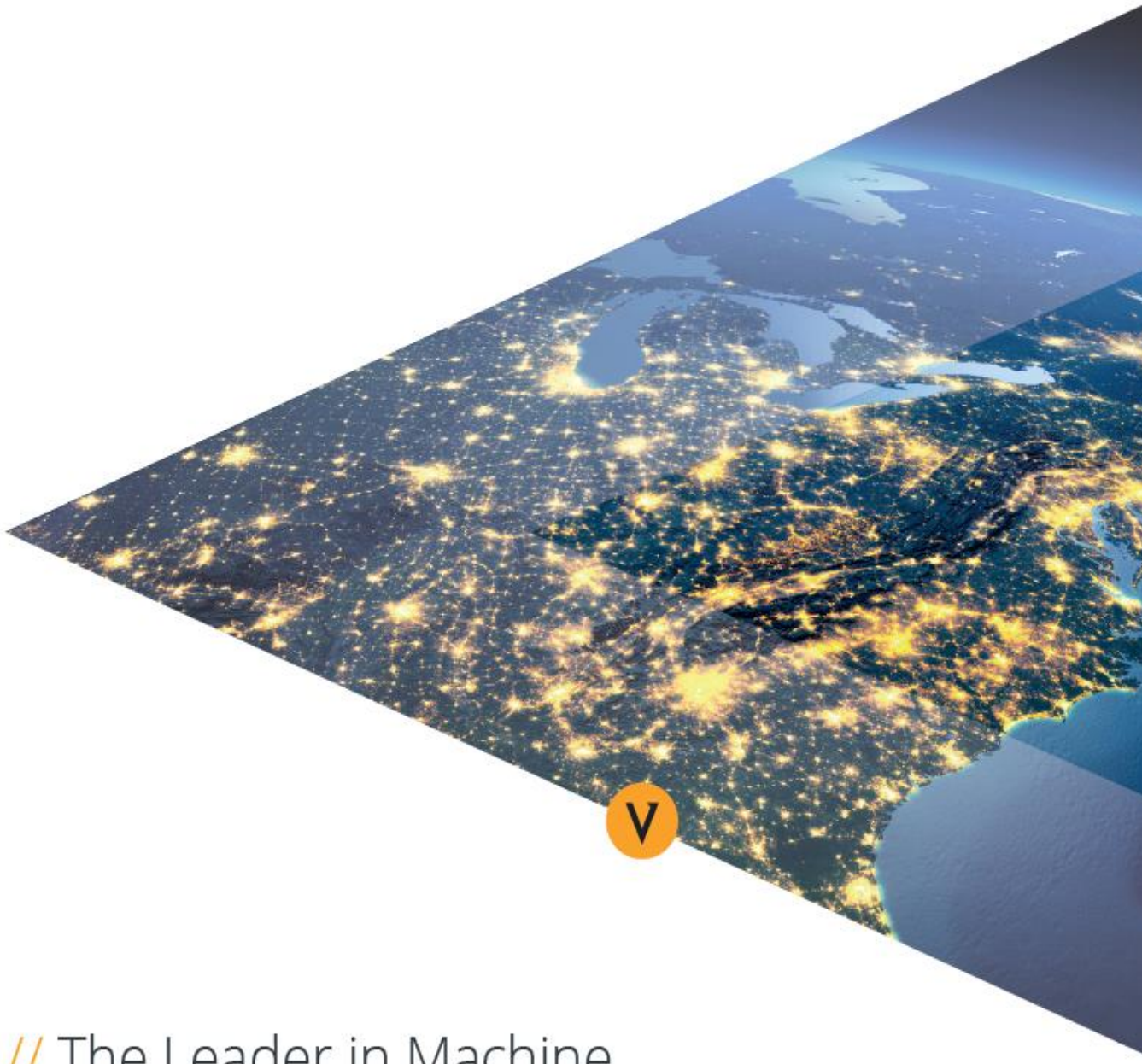
VENAFI®

Imperva Web Application Firewall (WAF) Installation and Usage Guide



// The Leader in Machine Identity Protection

VENAFI®

Contents

// Document Control

Version	Date	Author	Description
1.0.0	10/13/2020	Brant Peery	Initial release

// Introduction

Imperva is a cloud web application firewall that is used to protect websites against attacks. One of the features is site forwarding. The site forwarding feature can use custom certificates what will be served with the ssl connection to the site. Using this driver, all these site certificates can be managed by TPP. It allows for discovery of all sites and certificates associated with an API key. It also allows for the external creation and subsequent upload to an Imperva protected site.

// Assumptions and Constraints

// Assumptions

1. A valid Imperva API key is available that has access to all the sites that TPP will manage

// Installation

The modules are delivered in the format of a zip file containing the script and documentation. This is a single file with a name *ImpervaWAF <version>.zip*.

These instructions need to be followed on each Venafi server that can process logs

1. Unzip the file to a temp location
2. Copy the ImpervaWAF.ps1 file to <Venafi install>\Scripts\AdaptableLog

// Confirmation of Installation

To confirm successful installation of the package, perform the following quick checks:

- Navigate to <Venafi install root>/ and confirm the existence of
    - /Scripts/Adaptable Log/ImpervaWAF.ps1

// Overview of Application

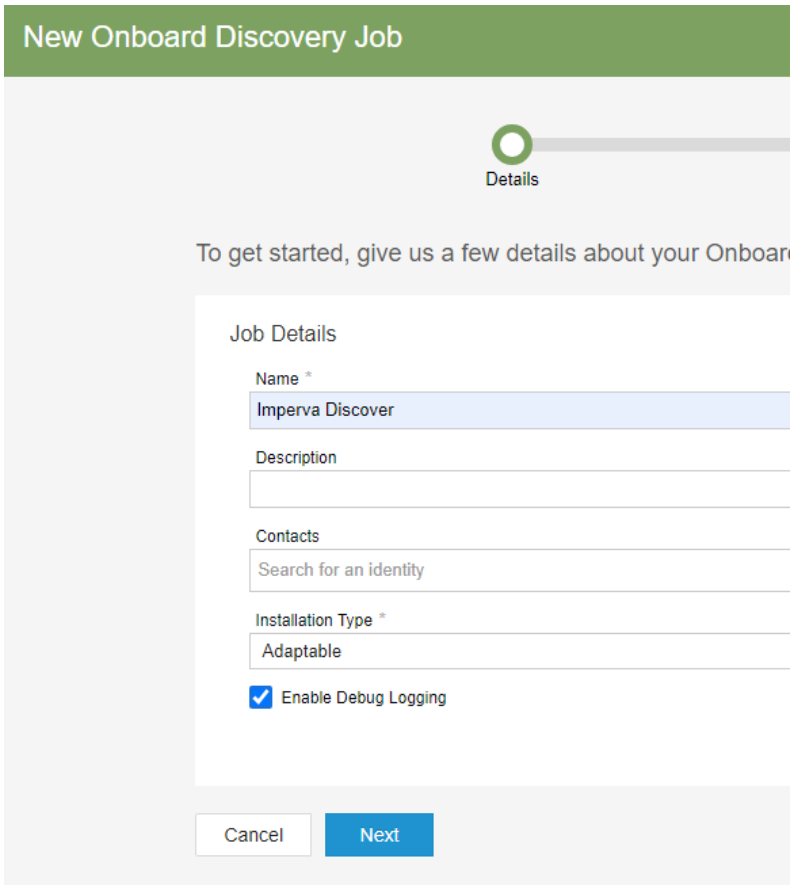
The driver handles two TPP stages

- Install-Certificate: It will push a certificate to the custom certificate settings section of the Imperva site.
- Discover-Certificates: It will call the /v1/sites/list endpoint in Imperva to get a list of all the sites for an account. It will then connect to each site and get the ssl certificate if it is served one. These are sent back to the discovery job to be handled by TPP.

// Configuration Steps

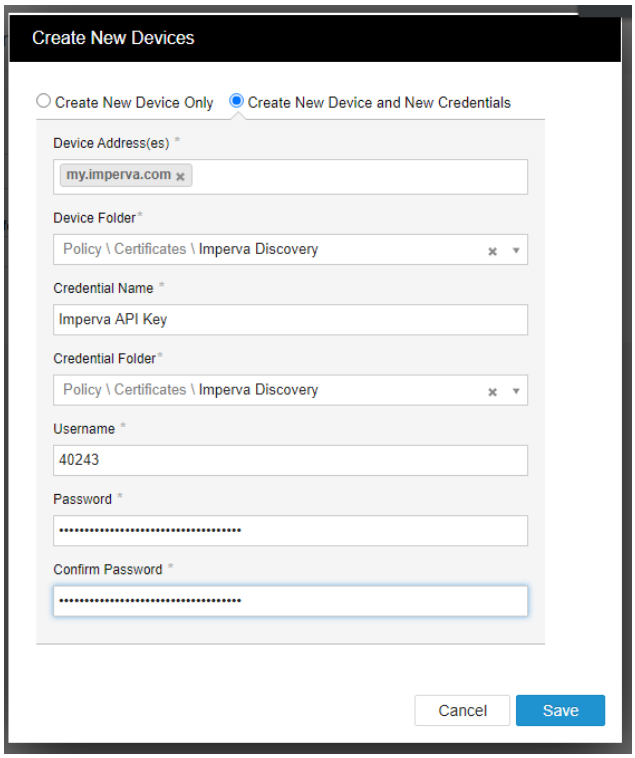
1. Open Aperture and go to Jobs

2. Add a new Onboard Discovery Job

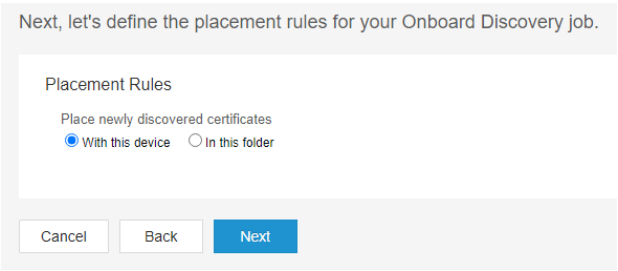


3. Make sure you select adaptable as the Installation Type.

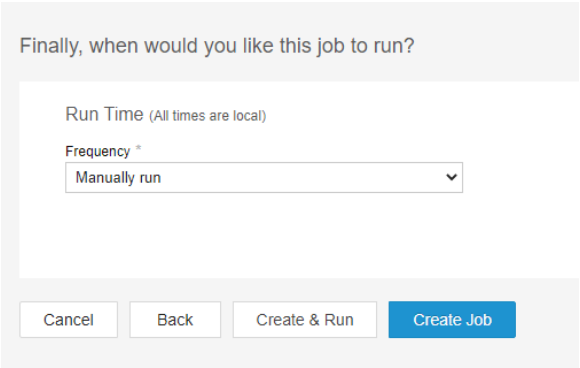
4. In the Devices to scan box, select Create New Devices



5. You can create your credential at the same time. Use the API key ID and password.
6. Click next and then select the placement rules. Click Next when done

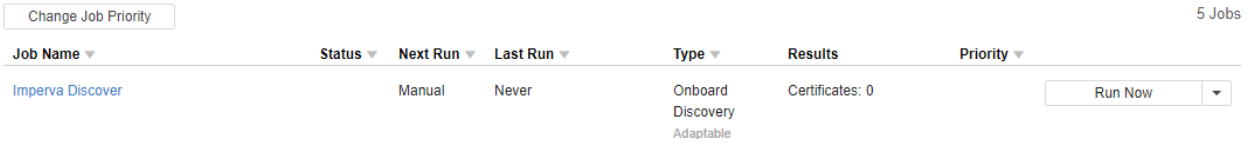


7. Select the run frequency.

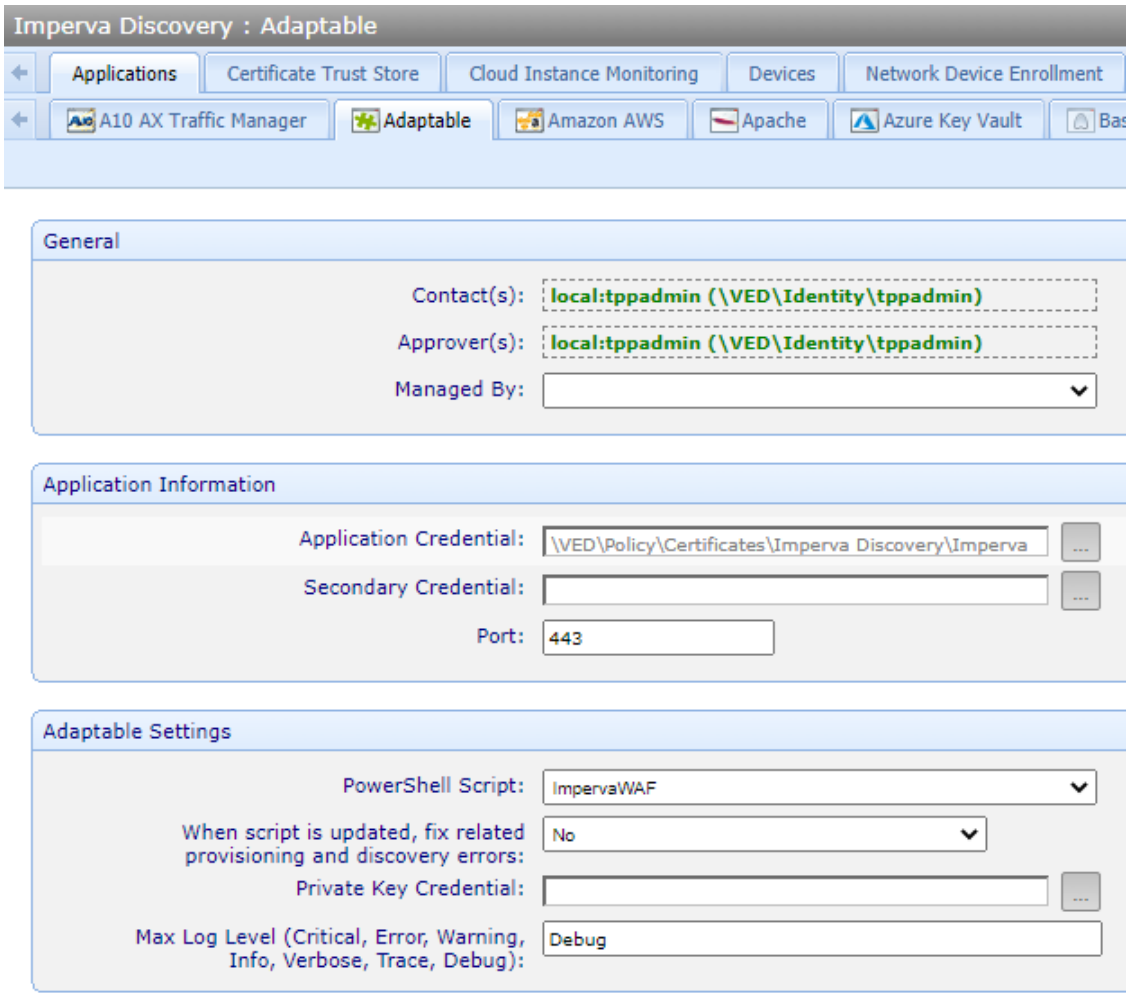


   a. Open the applications->Adaptable tab

8. Once done, check to make sure the job is in the job list



9. Now we have to set up the adaptable app script.
    a. Switch to VedAdmin so you can set the policy values on the discovery folder you selected for the device we just created



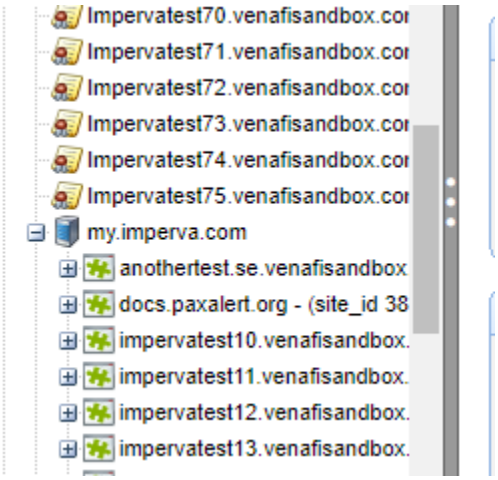
    b. Pay special attention to the Adaptable Settings section

10. Click save.

// Test the system

Run the job via the manual Run Now button. You should see all your Imperva certificates get imported into the directory selected in the setup of the job. The applications will also automatically be created on

the device object set up in step 4.



// TPP Log Events

Log Event	Description
There are no new custom TPP log events in the VSE	

// Uninstall

To uninstall the adaptable driver, the driver must be removed from the folder *<Venafi install root>/Scripts/AdaptableApp/ImpervaWAF.ps1*. Once that is done, all references to it by adaptable app objects in TPP must be changed in TPP to a different script.