ClearPass Integration with OPSWAT MetaAccess

aruba

a Hewlett Packard Enterprise company

ClearPass

TechNote

Change Log

Version	Date	Modified By	Comments
0.1	April 2018	Dennis Boas	Draft TechNote
1.0	May 2018	Dennis Boas	First Published Version

Copyright

Open Source Code

This product includes code licensed under the GNU General Public License, the GNU Lesser General Public License, and/or certain other open source licenses. A complete machine-readable copy of the source code corresponding to such code is available upon request. This offer is valid to anyone in receipt of this information and shall expire three years following the date of the final distribution of this product version by Hewlett- Packard Company. To obtain such source code, send a check or money order in the amount of US $10.00 to:

Hewlett-Packard Company
Attn: General Counsel
3000 Hanover Street
Palo Alto, CA 94304
USA

Please specify the product and version for which you are requesting source code. You may also request a copy of this source code free of charge at **HPE-Aruba-gplquery@hpe.com**.

Contents

a Hewlett Packard Enterprise company

www.arubanetworks.com
3333 Scott Blvd
Santa Clara, CA 95054
Phone: 1-800-WIFI-LAN (+800-943-4526)
Fax 408.227.4550

Introduction

This TechNote covers how to deploy and configure the ClearPass OPSWAT MetaAccess extension. The extension integrates ClearPass with the OPSWAT MetaAccess server for the retrieval of endpoint device and security posture information. OPSWAT MetaAccess provides real time posture information from endpoints agents to the MetaAccess server. The data is then used to assess the endpoint's security posture.

Use Case

This version of the Extension provides the initial client validation when authorizing the client (end system) for network access. The MetaAccess server is configured in ClearPass as an Authorization source. When an endpoint authenticates to ClearPass it will be authenticated and ClearPass can then request posture information from the MetaAccess server to make an informed endpoint authorization decision.

OPSWAT is an authorization source and it will not save details in endpoints database

Software Requirements

MetaAccess

A configured OPSWAT MetaAccess v1.0.0 or better deployment

ClearPass

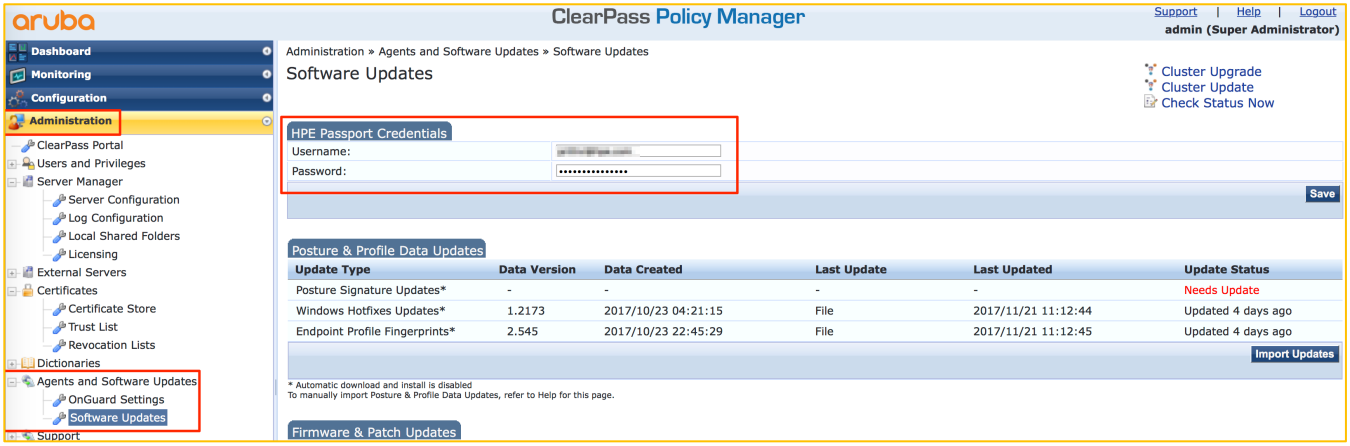
The minimum software version required for ClearPass is 6.7. ClearPass runs on hardware appliances with pre-installed software or as a Virtual Machine under the following hypervisors. Hypervisors that run on a client computer such as VMware Player are not supported.

- VMware ESXi 5.5, 6.0, 6.5 or higher
- Microsoft Hyper-V Server 2012 R2 or 2016 R2
- Hyper-V on Microsoft Windows Server 2012 R2 or 2016 R2
- KVM on CentOS 6.6, 6.7, or 6.8.

Access to the Extension Store

Access to the Extension Store to download Extensions is simplified in ClearPass 6.7. The ability to download extensions from the store and to validate support entitlement for access to the Software Updates Portal (e.g. Posture & Profile Data Updates, Software Updates, & Skins) now uses the HPE Passport account credentials that are associated with the customers' ClearPass licenses. This is configured where previously the subscription-id was defined, under **Administration -> Agents and Software Updates -> Software Updates** as shown below. Ensure you enter your HPE Passport credentials to enable Extension download capabilities.

Figure 1: *Entering HPE Passport Credentials*



Installation and Deployment Guide

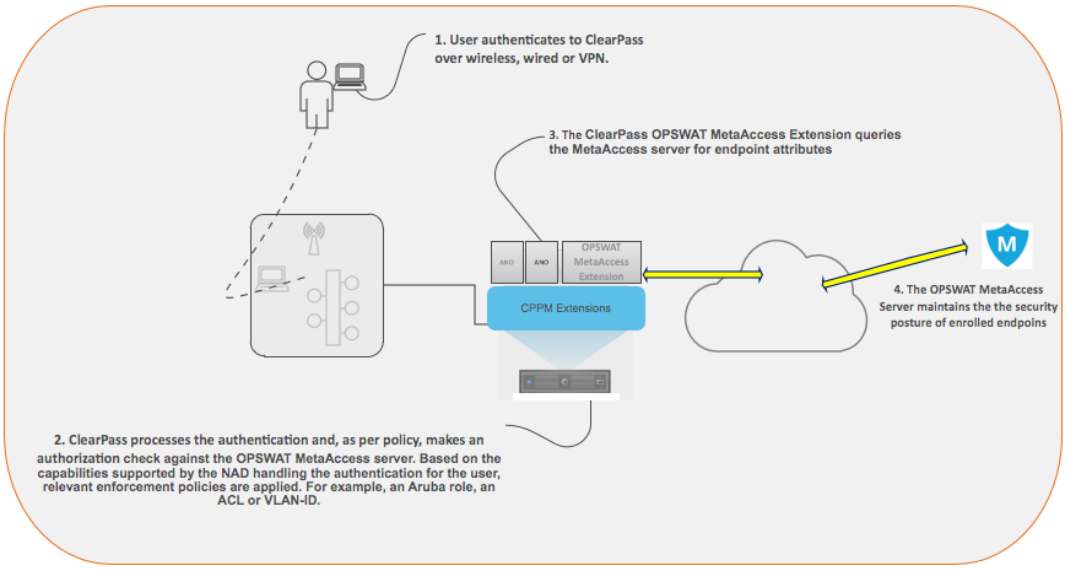
The generic ClearPass installation and deployment guide is located here:

https://support.arubanetworks.com/Documentation/tabid/77/DMXModule/512/Command/Core_Download/Default.aspx?EntryId=28321

Pictorial View of the Integration

The diagram below shows a pictorial overview of the components and how they interact with each other.

Figure 2: Pictorial view of ClearPass Policy Manager integration with OPSWAT MetaAccess Server



Extension Support in ClearPass 6.7

With the release of 6.7, several new features have been added to enhance the functionality of the Extension Framework. Previously all installation and operations required use of the API Explorer to interoperate with the Extension and the underlying framework. Now this functionality has been exposed with a new GUI. The GUI is accessed from within the Guest UI and is shown below, **Administration -> Extensions.**

Extensions and IP address configuration support

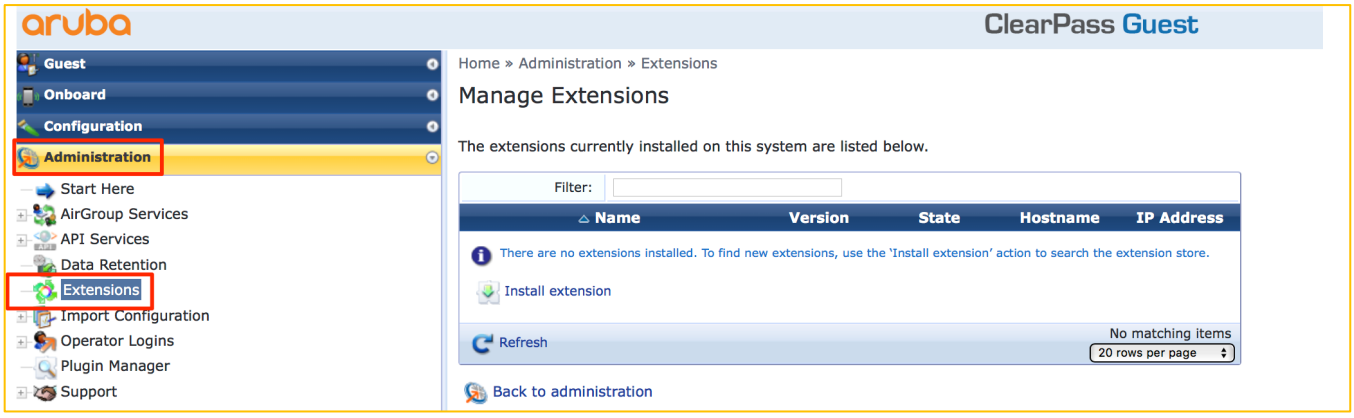
The other major additions in the 6.7 release is the ability to define the Extension framework base IP network and statically define the IP address of the individual extensions. The latter being useful when deploying Extensions in a cluster and the requirement for a fixed IP address for the same extension across a cluster regardless of which ClearPass node or nodes it is installed on.

Extensions and proxy support

Prior to 6.7 support for Proxy was limited to the installation of the Extensions, starting in ClearPass 6.7, Extensions now support communications with 3rd parties via a Proxy. This adds incremental Proxy functionality. If a Proxy is defined in ClearPass Policy Manager, then an Extension will use that configuration.

Note that the Policy Manger Proxy configuration is ONLY read at by the Extension at installation time. If the proxy configuration is changed in Policy Manager, then the extension must be re-installed, so the new settings are re-read and bonded to the extension.

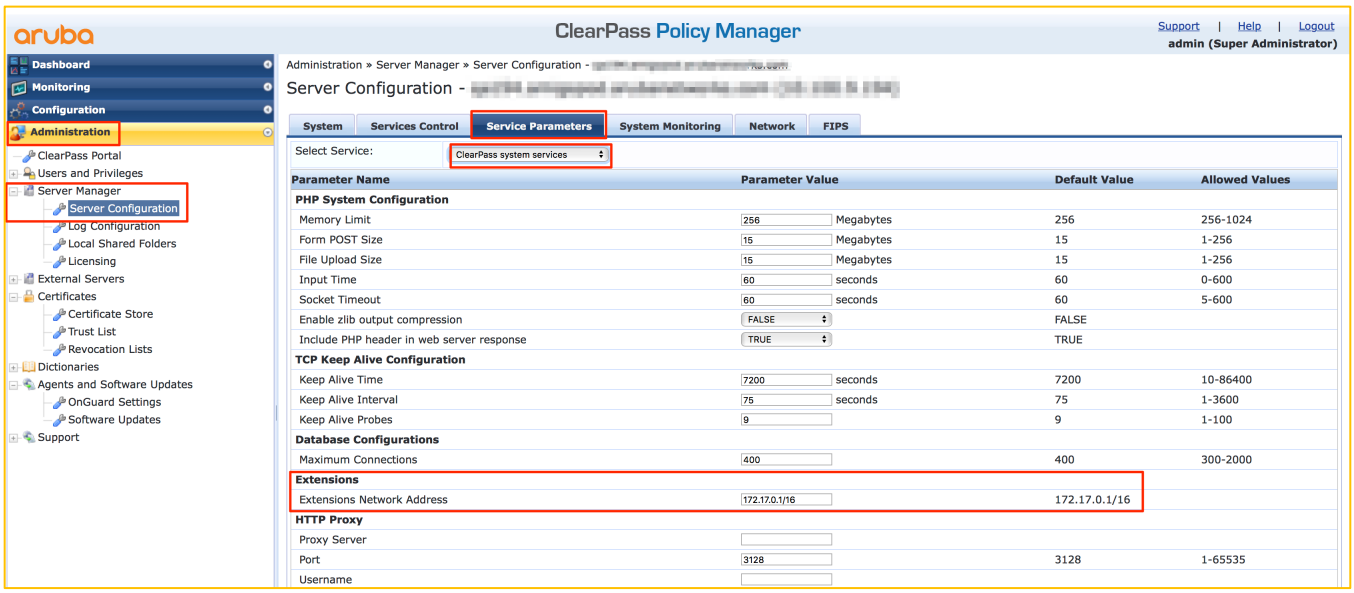
Figure 3: *Extension Framework GUI*



Configuring the base Extension IP subnet, this is defined within Policy Manager as shown below under **Administration -> Server Manager -> Server Configuration [chose your node] Service Parameters [ClearPass system service].** The default is 172.17.0.1/16, this address is the non-routed address of the ClearPass node itself. The IP addresses range for the extensions are based upon the network prefix used.

Note that the subnet defined here for the Extension framework must be one of the following 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16.

Figure 4: *Defining the base IP SUBNET and LOCALHOST for the Extensions Framework*



Note that changing the Extension base IP address will require the Extension service to be restarted.

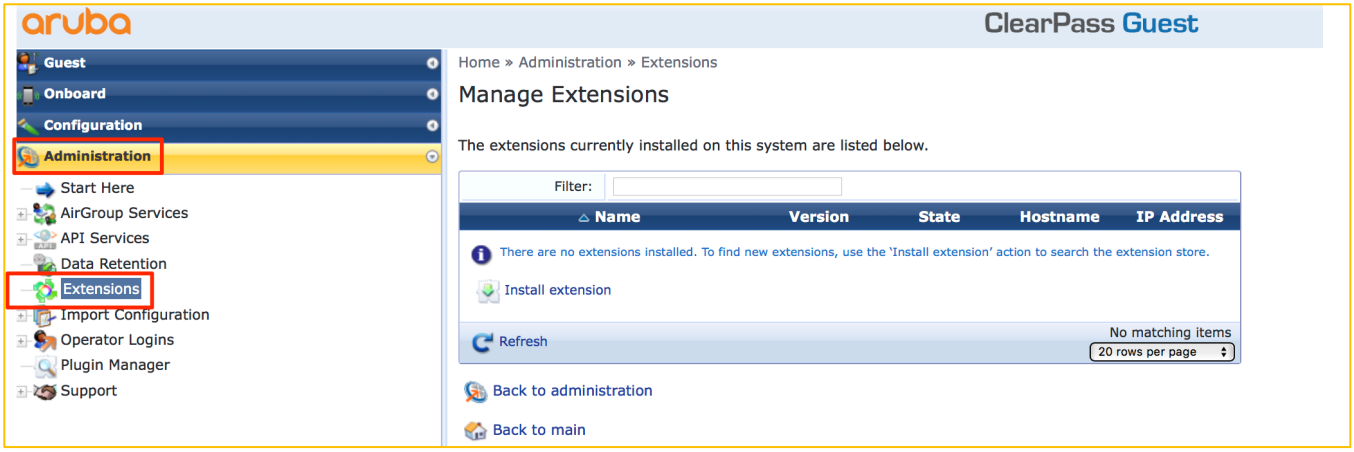
Changing the Extension Network Address range is necessary, if either the MGMT or DATA interface are also using an address in the extension default range of 172.17.x.x/12. Set the new Extension IP range as needed and restart the Extension service for this to take effect.

Extension Installation Using GUI in 6.7+

Starting in ClearPass 6.7, a Graphical User Interface was introduced to make the process of interacting with the Extension Framework easier. It provides a simplified and intuitive experience. To access the Extension GUI, from the **Guest System**, under **Administration** find the **Extension** User Interface as shown below.

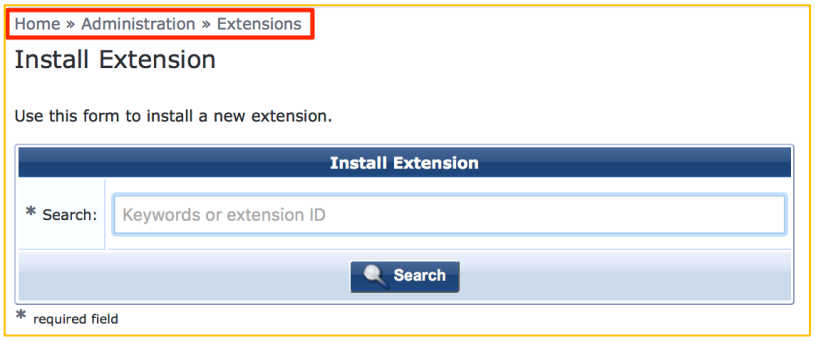
Note: The OPSWAT MetaAccess extension is only available for installation on ClearPass 6.7+

Figure 5: *Extensions Framework GUI*



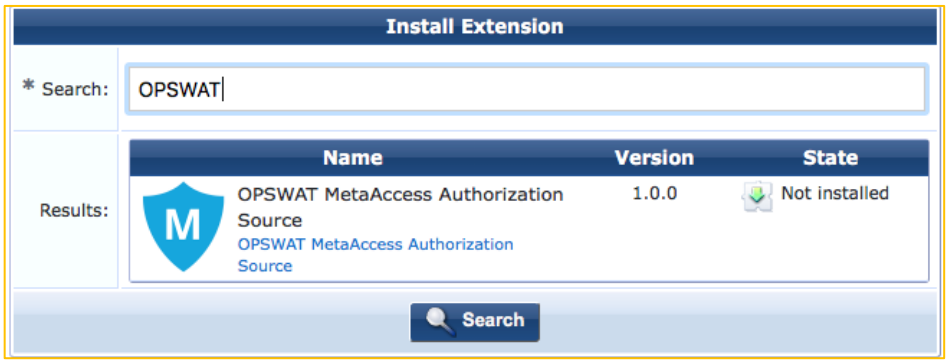
From here click on '**Install Extension'**, and the search box below appears.

Figure 6: *GUI Extension Installation*



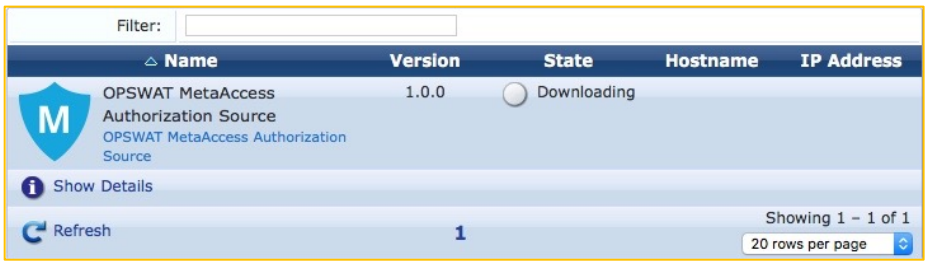
Enter either the Store-ID, or enter the name or partial name of the Extension, and click on 'Search', an example below.

Figure 7: *GUI Extension Search*



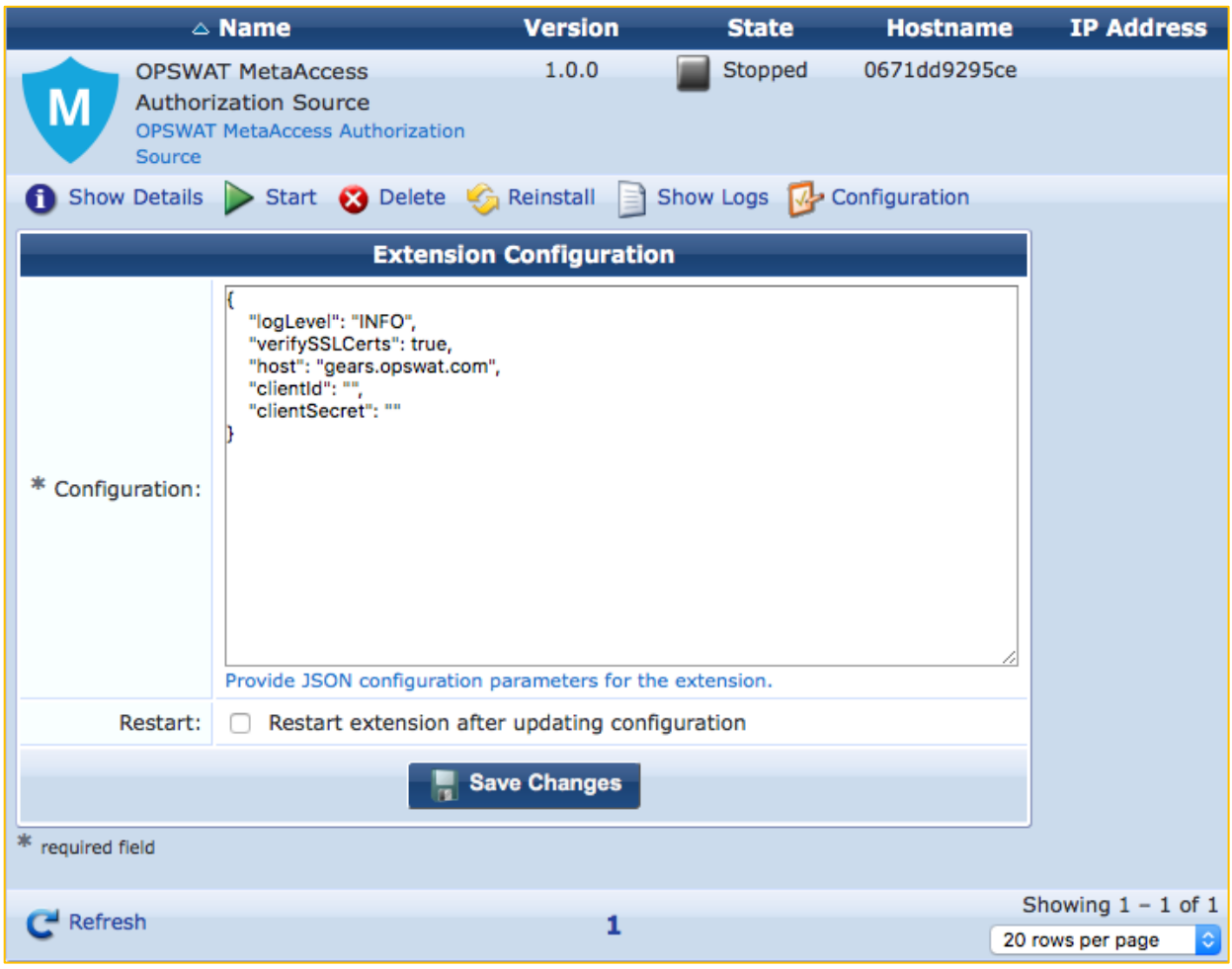
Click on the Extension and then the Install option

Figure 8: *GUI Extension Downloading*



After the extension has been installed review the extension configuration as necessary and adjust as needed. Notice the options to Start, Delete, Reinstall, Show Logs and the option to review and set the Extension configuration.

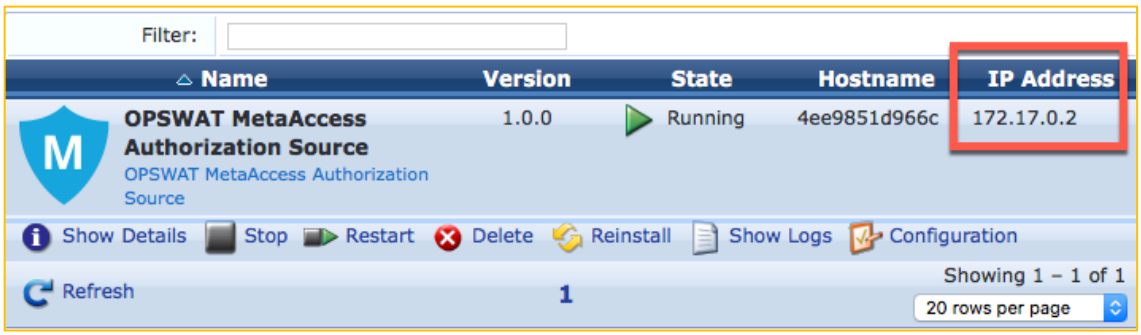
Figure 9: *GUI reviewing and setting the Extension Configuration*



A copy of the default MetaAccess Extension is shown above, this will need to be modified for your deployment. Add the "Client Id" and "Client Secret". For installation verification and troubleshooting change "Log Level" to Debug

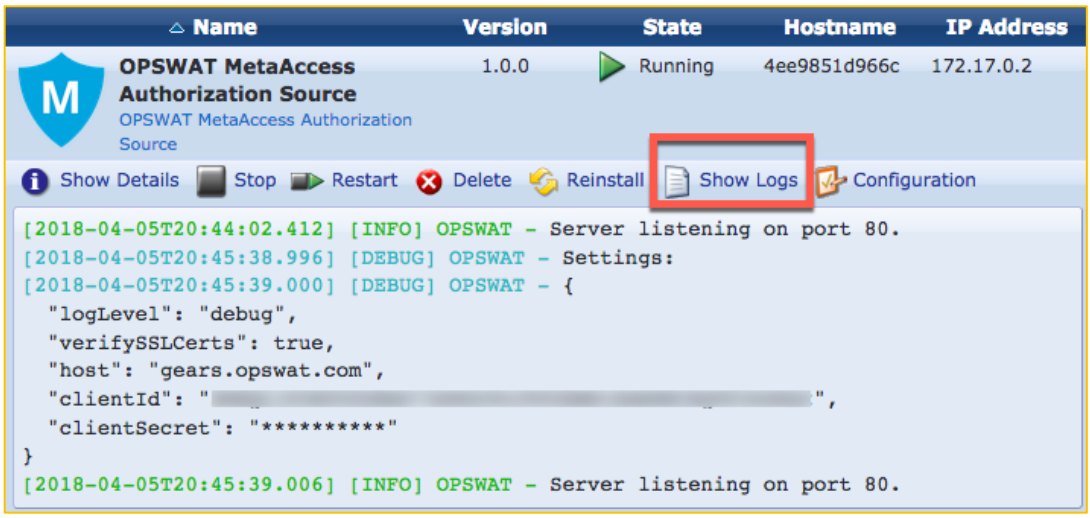
After the extension is started record the IP Address assigned to the Extension, this will be needed later to add the extension as an Authentication Source

Figure 10: *Record IP Address of Extension*



Click “Show logs” to verify extension start up

Figure 11: *Show Logs*



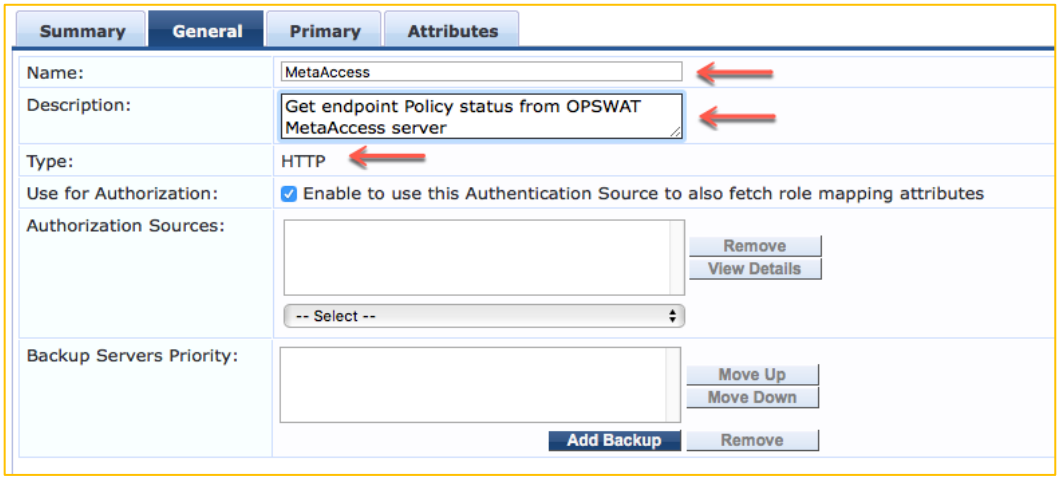
ClearPass Policy Manager Configuration

Following the deployment and configuration of the ClearPass Extension, the next step is to configure a ClearPass HTTP authorization source for the OPSWAT MetaAccess Extension. The HTTP authorization source is the conduit between the extension and ClearPass Policy Manager. It's through the authorization source that the OPSWAT MetaAccess endpoint attributes are exposed to Policy Manager so they can be used in an enforcement policy.

The first step is to add the authorization source. Under Configuration -> Authentication -> Sources, Click

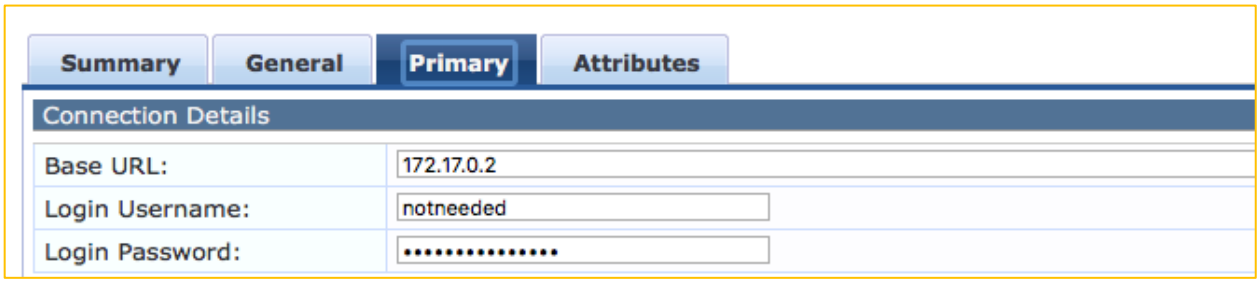
Add and choose type HTTP.

Figure 12: *Add Authorization Source*



Add a Name and description for the Authentication Source and enable it to fetch role mapping attributes. Click Next and on the Primary Tab, provide the IP Address of the extension you recorded previously.

Figure 13: *Add Extension IP Address*

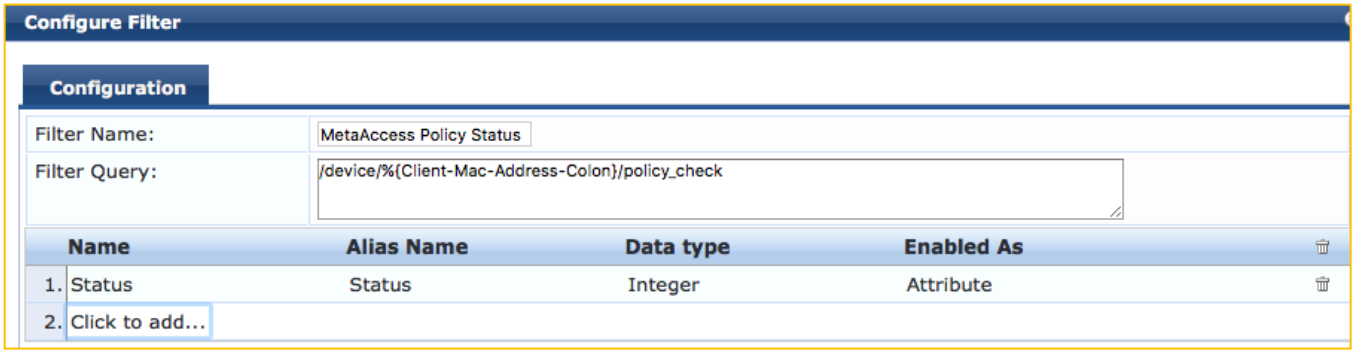


NOTE

The Base URL is the IP address previously recorded when the extension was started. The Login Username and Password can be set to ANYTHING; they are not used by this extension but the parameters are mandatory.

Click on Next. This will advance you to the Attributes Tab where you need to provide the authorization Query Filter and attributes. Click on Add More Filters. Provide a Name for the filter and then add the Filter Query.

Figure 14: *Add Filter Query*



It's extremely important that the Filter Query is defined correctly. This is the query string that is sent to the OPSWAT MetaAccess Extension requesting context about the endpoint. The query is indexed off the MAC Address of the authenticating endpoint. For ease in copying, the Filter Query is provided here.

/device/%{Client-Mac-Address-Colon}/policy_check

The Policy Check request returns one of four stratus values that can be used for Authorization

Status values are:

0 – the endpoint is in compliance with MetaAccess account's policies

1 – the endpoint is not in compliance with MetaAccess account's policies

2 – the endpoint is not found, it means that the endpoint does not have the MetaAccess installed

3 – the endpoint is still sending information to MetaAccess and not yet completed

The OPSWAT MetaAccess Extension supports two Filter Queries

/device/%{Client-Mac-Address-Colon}/policy_check

/device/%{Client-Mac-Address-Colon}

Both filters return a larger amount of information. Not all of the data is relevant to making a security policy decision about the endpoint. Carefully choose which attributes are required within your enforcement profile. The following links document the returned attributes.

https://onlinehelp.opswat.com/metaaccess/Device_Details.html

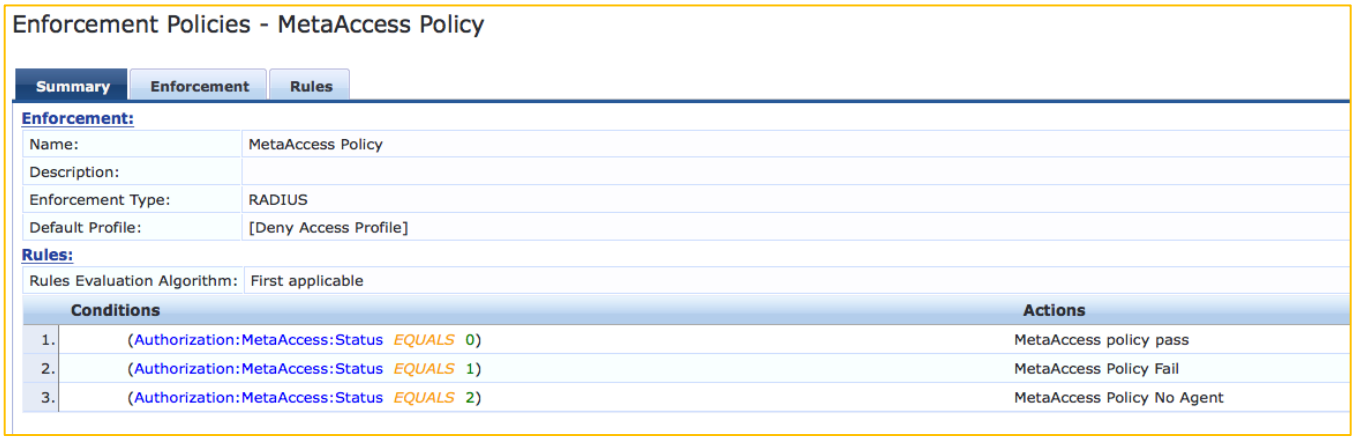
https://onlinehelp.opswat.com/metaaccess/Device_Policy_Check.html

Choose the attributes that are relevant to your security posture checks.

Using OPSWAT MetaAccess Status in an Enforcement Policy

This is an example of a ClearPass enforcement policy using the endpoint status returned by the MetaAccess server.

Figure 16: Add Enforcement Policy



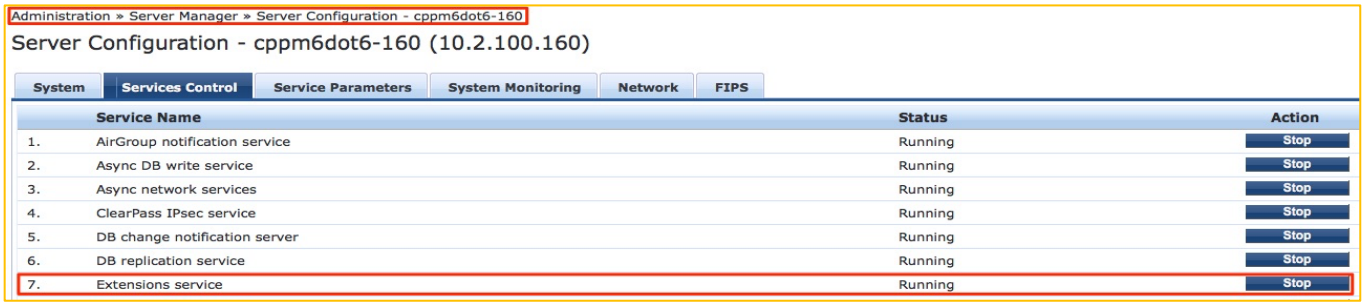
Appendix A – Additional Diagnostics & Support

Extension Service

The ClearPass Extension is supported by a new system service that was initially added in 6.6. This service should be running. Note that restarting this service will affect **all** deployed and running extensions.

To check on the state and to restart the service, go to **Administration > Server Manager > Server Configuration [select a cppm node] > Service Control.** From here start/stop the extension service. By default, this service is automatically started.

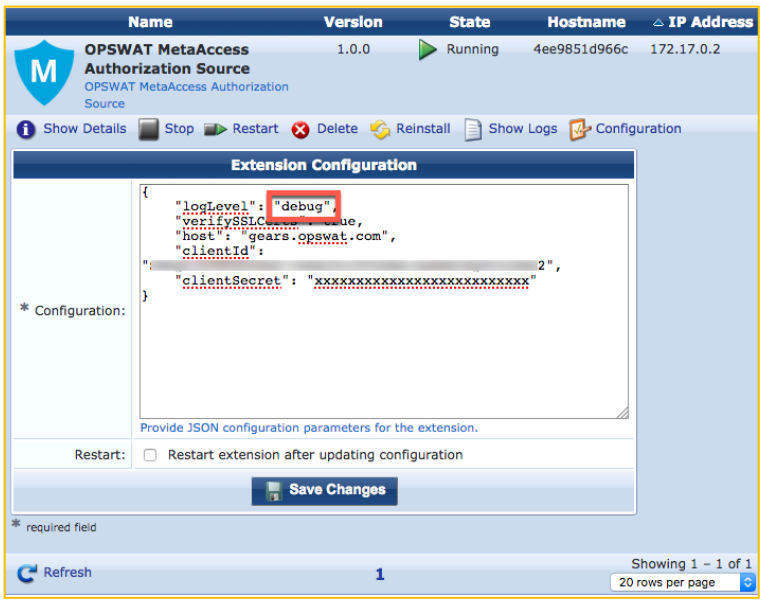
Figure 17: *Checking on Extension service and how to start/stop the service*



Extension Logs/Debugging

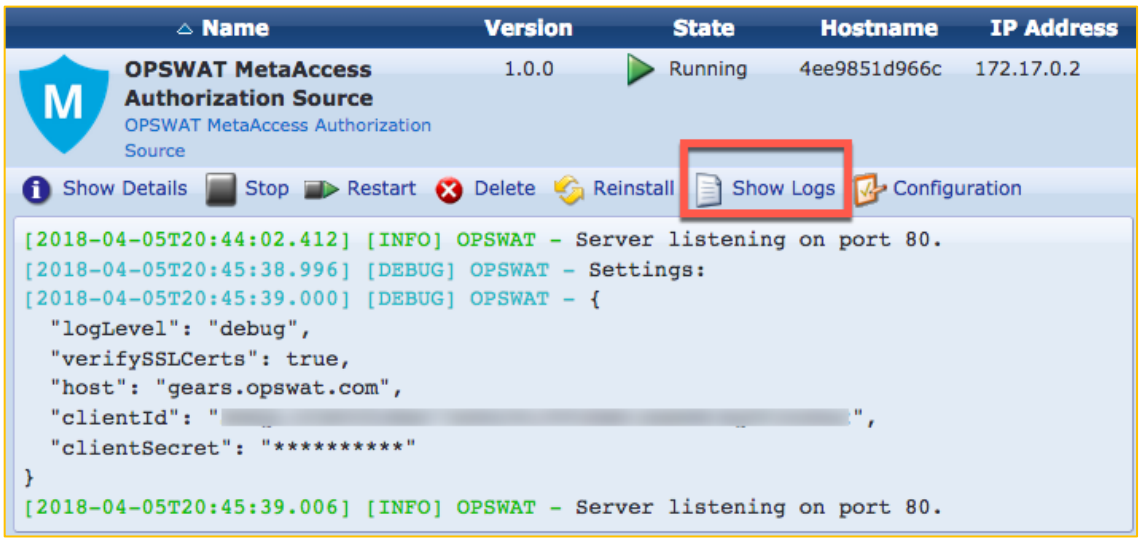
If there is a need to access the logs from inside the Extension, In the 6.7 GUI change the config and restart the extension as shown below.

Figure 18: *Using the GUI to change the "debug" level*



Logs can then be viewed from the '**Show Logs**'.

Figure 19: *Show Logs*



Accessing Extension logs within ClearPass 'Collect Logs'

In addition to the logging of messages that be examined in the extension as shown above, it's possible to configure the extension to log messages so that they can be collected and examined via the Policy Manager **'Collect Logs'** system function. This is extremely useful for Aruba TAC.

If there is a requirement for Aruba TAC to investigate a system issue, one of the items they regularly ask for is the system logs to aid with their diagnostic investigation. The ClearPass extension can write its logs such that they are available and can be collected with all other system diagnostics information when **the 'Collect Logs**' function is run. Remember by default, the logLevel is set to INFO but TRACE, DEBUG, INFO, WARN, ERROR, FATAL can also be set. Any of the levels will display the information for the selected state and lower, so if INFO is selected it will show messages for INFO, WARN, ERROR, FATAL.

After the Logs have been collected and exported from the system, expand the GZ file and locate the extension logs in the following location '**PolicyManagerLogs->extension'** as shown below.

Figure 20: *Extension logs location in 'Collect Logs' diagnostic GZ file*