Microsoft Defender ATP
Change Log

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Modified By</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>2020-01</td>
<td>March 2020</td>
<td>Anish Pansare</td>
<td>Initial Release</td>
</tr>
</tbody>
</table>

Copyright

©Copyright 2020 Hewlett Packard Enterprise Development LP.

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

Introduction and Overview.................................................................................................................................................. 5
Pictorial View of the Integration......................................................................................................................................... 6
Software Requirements.......................................................................................................................................................... 6
Installation and Deployment Guide....................................................................................................................................... 6
Access to the Extension Store............................................................................................................................................. 7
New Extension Support in ClearPass 6.7+............................................................................................................................. 7
  Extensions and IP address configuration support........................................................................................................... 7
Defender ATP Extension Installation and Configuration.................................................................................................. 10
Defender ATP configuration............................................................................................................................................... 22
Appendix A – Additional Diagnostics and Support............................................................................................................. 21
  The Extensions Service.................................................................................................................................................... 21
  Extension logs and debugging.......................................................................................................................................... 21
  Accessing extension logs within ClearPass ‘Collect Logs’ .............................................................................................. 26
Figures

Figure 1: Pictorial view of ClearPass Policy Manager integration with Defender ATP ................................................................. 6
Figure 2: Entering HPE Passport credentials .......................................................................................................................... 7
Figure 3: Extension framework GUI ............................................................................................................................................ 8
Figure 4: Defining the base IP SUBNET and LOCALHOST for the Extensions framework .......................................................... 9
Figure 5: Extensions framework GUI ............................................................................................................................................ 10
Figure 6: GUI Extension search ..................................................................................................................................................... 10
Figure 7: GUI Extension install .................................................................................................................................................... 11
Figure 8: GUI Extension configuration at install time ................................................................................................................ 11
Figure 9: Extension configuration parameters ........................................................................................................................ 12
Figure 10: Creating an Admin user on ClearPass ........................................................................................................................ 13
Figure 11: GUI review and setting the Extension configuration ................................................................................................ 14
Figure 12: Log validation ............................................................................................................................................................... 14
Figure 13: Attributes fetched ....................................................................................................................................................... 15
Figure 14: Example of an Enforcement Policy utilizing attributes returned from Defender ATP .................................................. 16
Figure 15: Example Context Server Action ................................................................................................................................ 16
Figure 16: Checking on the extensions service and how to start/stop the service .................................................................. 19
Figure 17: Using the GUI to change the DEBUG level ................................................................................................................ 19
Figure 18: Extension logs location in 'Collect Logs' diagnostic GZ file ...................................................................................... 27
Introduction and Overview

Microsoft Defender Advanced Threat Protection is a unified platform for preventative protection, post breach detection, automated investigation and response.

Microsoft Defender ATP includes risk-based Threat & Vulnerability Management to discover, prioritize and automate mitigation of vulnerabilities and security misconfiguration. The platform also provides security admins tools to reduce the attack surface without limiting a user’s productivity. Its behavioral-based and cloud-powered threat and malware protection prevents sophisticated and never-before-seen threats from impacting devices.

Deep optics into the operating system, including memory and kernel, help to detect 0-days, advanced attacks, and data breaches. Microsoft Defender ATP accelerates remediation by automatically investigating alerts and remediating threats – allowing security teams to go from alert to remediation in minutes - at scale.

This integration guide covers the deployment and configuration of ClearPass Policy Manager to interface with Defender ATP. The integration leverages Defender ATP APIs to obtain attributes associated with an endpoint. It provides an ability to ingest all device details from a customer tenant into the ClearPass endpoints database. The contextual data consumed into ClearPass can then be leveraged to drive granular access policy and segmentation workflows.
**Pictorial View of the Integration**

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

*Figure 1: Pictorial view of ClearPass Policy Manager integration with Defender ATP*

---

**Software Requirements**

The minimum software version required for ClearPass is 6.7.2. At the time of writing, ClearPass 6.8.4 is the latest available and recommended release. Any subsequent ClearPass software release will support this integration. ClearPass runs on either 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 vSphere Hypervisor (ESXi) 6.0, 6.5, 6.5 U1, 6.5 U2, 6.7, and 6.7 U1
- Microsoft Hyper-V Server 2012 R2, Microsoft Hyper-V Server 2016, Microsoft Hyper-V Server 2019
- Amazon EC2
- KVM on CentOS 7.5 or later
Installation and Deployment Guide

This document assumes your ClearPass environment is already configured and operational. If you require assistance with basic deployment, refer to the following deployment guide:


Access to the Extension Store

Access to the Extension Store to download extensions was 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 2: Entering HPE Passport credentials

New 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 extension installation and operation tasks 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 are 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 web proxy support

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

The Policy Manager web proxy configuration is ONLY read by the extension at installation time. If the web 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 10.0.0/8, 172.16.0.0/12 or 192.168.0.0/16.
Figure 4: Defining the base IP SUBNET and LOCALHOST for the Extensions framework

Changing the extension base IP address will require the extension service to be restarted.

Changing the “Extensions 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/16. Set the new network address range as needed and restart the extension service for this to take effect.
Microsoft Defender ATP Extension Installation and Configuration

Starting in ClearPass 6.7, a Graphical User Interface (GUI) was introduced to make the process of interacting with the extension framework easier. To access the extension GUI, from the Guest System, under Administration find the Extension User Interface as shown below.

**Figure 5: Extensions framework GUI**

![Image of the Extensions framework GUI](image)

From here, click on 'Install Extension', and the search box below appears. Enter the extension name and click on Search.

**Figure 6: GUI Extension search**

![Image of the GUI Extension search](image)

Starting 6.7, in a cluster environment an extension can be installed on the subscriber nodes directly.

---

**NOTE**

Starting 6.7, in a cluster environment an extension can be installed on the subscriber nodes directly.
Click on the Extension and then the **Install** option

**Figure 7: GUI Extension install**

![GUI Extension install](image)

Optionally set a specific IP address for the Extension if required. It will automatically pick an IP address if not assigned.

**Figure 8: GUI Extension configuration at install time**

![GUI Extension configuration at install time](image)
After the Extension has been installed, review the configuration and adjust as needed. There are options to Start, Delete, Reinstall or Show Logs and the option to edit and set the Extension configuration.

The default configuration used for Microsoft defender ATP extension is below:

```
{
    "logLevel": "INFO",
    "verifySSLCerts": true,
    "resourceId": "https://api.securitycenter.windows.com",
    "baseUrl": "https://api.securitycenter.windows.com/api/",
    "clientId": "[Client ID]",
    "clientSecret": "*******",
    "tenantId": "[Tenant ID]",
    "syncAllOnStart": false,
    "syncSeenSinceLastUpdateOnly": false,
    "enableSyncAll": false,
    "syncAllSchedule": "0 2 * * 6",
    "machinePageSize": 1000,
    "cppmUserName": "[User Name]",
    "cppmPassword": "*******",
    "enableStats": "true"
}
```

Each of the attributes are explained in the table below in detail.

**Figure 9: Extension configuration parameters**

<table>
<thead>
<tr>
<th>Configuration attribute</th>
<th>Description</th>
<th>Example/Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>LogLevel</td>
<td>Logging level for troubleshooting</td>
<td>&quot;DEBUG&quot;, &quot;INFO&quot;, &quot;WARN&quot;, &quot;ERROR&quot;</td>
</tr>
<tr>
<td>verifySSLCerts</td>
<td>Should SSL certificates be validated when communicating with Defender ATP.</td>
<td>true or false</td>
</tr>
<tr>
<td>resourceId</td>
<td>The token resource ID. This should generally be <a href="https://api.securitycenter.windows.com">https://api.securitycenter.windows.com</a></td>
<td>Example: api.securitycenter.windows.com</td>
</tr>
<tr>
<td>baseUrl</td>
<td>The API base URL. The default is <a href="https://api.securitycenter.windows.com/api/">https://api.securitycenter.windows.com/api/</a> but region-specific URLs can be used as well.</td>
<td><a href="https://api.securitycenter.windows.com/api/">https://api.securitycenter.windows.com/api/</a></td>
</tr>
</tbody>
</table>
When leveraging the sync capabilities of the Extension to get the device attributes from Defender ATP, use the attribute `enableSyncAll` and specify `syncAllSchedule`. These 2 attributes are leveraged for periodic poll of endpoints from Defender ATP. The `syncAllOnStart` attribute can be leveraged as well to sync everything upon the start of the extension. When `syncSeenSinceLastUpdateOnly` is set to true, the sync all process will limit the updates to machines that have been seen since the last update run. When `enableStats` is set to true, extension statistics pertaining to CPU and memory usage, outgoing HTTP(s) requests, API status codes. Check Appendix A for more details.

The `clientId`, `clientSecret` and `tenantId` are collected from inside the Defender system.

The `cppmUserName` and `cppmPassword` should be for a Network Administrator. The device profiling attributes obtained from Defender ATP need to be written into the endpoint repository leveraging the REST APIs which requires a Network Administrator account.

A ClearPass Network Administrator account can be created under Administration > Users and Privileges > Admin Users. Click on Add. A user with the following Privilege Level needs to be created.

Figure 10: Creating an Admin user on ClearPass
A Network Administrator privilege level is sufficient for the action of adding device profiling information into the endpoint database of ClearPass.

A copy of the Defender ATP Extension with the desired configuration is shown below, this has to be modified for your deployment. Include the `resourceId`, `baseUrl`, `clientId`, `clientSecret`, `tenantId`, `cppmUserName` and `cppmPassword` that will be specific to your environment.

Change or include any other values based on the description of each in the above table. Select **Restart** and click on **Save Changes** to restart the extension.

**Figure 11: GUI review and setting the Extension configuration**

![Extension Configuration](image)

After the configuration, click on **Start**. You can then check the logs under **Show Logs**.

**Figure 12: Log validation**

![Log validation](image)
The above log shows that the Extension has synced the endpoint data from Defender ATP. It syncs endpoint details at the time of starting the Extension and then regular updates are fetched at the interval specified by `syncAllSchedule`, if configured. Please note the IP address of the Extension. This will be used in the next section where we leverage the Defender ATP attributes during enforcement for real-time checks. A sample of endpoint attributes synced are shown below.

Figure 13: Attributes fetched

<table>
<thead>
<tr>
<th>Endpoint</th>
<th>Attributes</th>
<th>Device Fingerprints</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. MSFT DATP Agent Version</td>
<td>= 10.5850.17763.771</td>
<td></td>
</tr>
<tr>
<td>2. MSFT DATP Computer Dns Name</td>
<td>= desktop-hn5jbcq</td>
<td></td>
</tr>
<tr>
<td>3. MSFT DATP Exposure Level</td>
<td>= Medium</td>
<td></td>
</tr>
<tr>
<td>4. MSFT DATP First Seen</td>
<td>= 2020-01-22T22:24:49.4213345Z</td>
<td></td>
</tr>
<tr>
<td>5. MSFT DATP Health Status</td>
<td>= Active</td>
<td></td>
</tr>
<tr>
<td>6. MSFT DATP ID</td>
<td>= 76286d910c7a0911813b0925afd6b1648dcaf3</td>
<td></td>
</tr>
<tr>
<td>7. MSFT DATP Last External IP Address</td>
<td>= 104.36.248.13</td>
<td></td>
</tr>
<tr>
<td>8. MSFT DATP Last Seen</td>
<td>= 2020-02-22T01:55:32.4028489Z</td>
<td></td>
</tr>
<tr>
<td>9. MSFT DATP Last Update</td>
<td>= 2020-02-22 02:00:01</td>
<td></td>
</tr>
<tr>
<td>10. MSFT DATP MAC Addresses</td>
<td>= 8C16456C1DD3, 3BDEAD923C55, 3A0DEA923C54, 3BDEAD923C54</td>
<td></td>
</tr>
<tr>
<td>11. MSFT DATP OS Build</td>
<td>= 17763</td>
<td></td>
</tr>
<tr>
<td>12. MSFT DATP OS Platform</td>
<td>= Windows10</td>
<td></td>
</tr>
<tr>
<td>13. MSFT DATP OS Processor</td>
<td>= x64</td>
<td></td>
</tr>
<tr>
<td>14. MSFT DATP Rbac Group ID</td>
<td>= 0</td>
<td></td>
</tr>
<tr>
<td>15. MSFT DATP Risk Score</td>
<td>= None</td>
<td></td>
</tr>
</tbody>
</table>
Multiple use-cases exist for how the data that is returned from Defender ATP can be used in the Policy enforcement. In the example below, we are performing multiple checks:

1. Check if the device is found in the Defender ATP system. If it is not, redirect it to the captive portal. Create a helpdesk ticket for remediation.

2. Check when the device was last seen and the health status. If it is more than 7 days, redirect it to the captive portal and create a helpdesk ticket.

3. Check on machine tags in the Defender ATP and the OS platform.

4. Check on the exposure level and depending in that allow or deny access on the network.

**Figure 14: Example of an Enforcement Policy utilizing attributes returned from Defender ATP**

<table>
<thead>
<tr>
<th>Conditions</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. (Endpoint:MSFT DATP System Found NOT_EQUALS true)</td>
<td>Defender ATP - Redirect to Captive Portal</td>
</tr>
<tr>
<td>2. (Endpoint:MSFT DATP Last Seen NOT_EQUALS 2020-02-14T15:40:38.6104871Z) AND (Endpoint:MSFT DATP Health Status EQUALS Inactive)</td>
<td>Defender ATP - Quarantine VLAN, Defender ATP - Create Helpdesk Ticket</td>
</tr>
<tr>
<td>4. (Endpoint:MSFT DATP OS Platform EQUALS Windows10) AND (Endpoint:MSFT DATP Exposure Level NOT_BELONGS_TO Medium)</td>
<td>Defender ATP - Create Helpdesk Ticket, Defender ATP - Quarantine VLAN</td>
</tr>
</tbody>
</table>

Different companies will have different enforcement profiles and policies. The key takeaway here is to leverage the attributes received from Defender ATP to drive the policy engine into making different enforcement actions for the device as they authenticate on the network.

For all endpoint actions based on MAC address a lookup on the ClearPass Endpoint database is done to try and get the “MSFT DATP ID” from attribute values. If this value does not exist, the action will fail. More details on the machine actions can be found here: [https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/machineaction](https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/machineaction).
Use Cases

The extension can serve multiple use cases as described in the Introduction as well as the Pictorial. Each use case would require some further configuration based on the requirement. Microsoft Defender ATP allows below actions for a particular machine:

Microsoft Defender ATP allows below actions for a particular machine:

Below use case demonstrates how these actions can be achieved using ClearPass Policy Manager Extension and lists the available Context Server Actions.

Isolate an endpoint using Defender ATP APIs

ClearPass Policy Manager extension can call the Defender ATP APIs to isolate an endpoint. APIs can also be leveraged to unisolate an endpoint. Configuration for isolation includes 3 steps on ClearPass Policy Manager.

1. Define Endpoint Context Server
2. Add Context Server Action
3. Create an Enforcement Profile to trigger the action

Create a Context-Server as below. Point at the IP address of the extension, ensure you configure this as http.

Figure 15: Context-Server definition
Select the **Server Type** as “Generic HTTP”. The **Server Name** is the IP address of the extension. Once you enter that, the **Server Base URL** gets automatically populated and adds https to begin with. Ensure that you change this to **http** else the internal POST fails. Please note that this is an internal POST within ClearPass from the Policy Manager to the extension.

The next step is to define a Context Server Action within ClearPass Policy Manager which will internally POST to the extension. The extension will trigger an API call to Defender ATP and fetch the information associated with it which can be used for Authorization. The context server action allows us to define the HTTP Method, the URL and the JSON contents that will be used to post the mac access to the extension.

This can be added under **Administration > Dictionaries > Context Server Actions**. Click on **Add** and use the details below. All the other tabs are blank.

The URL used below has to match for the API calls to be successful. Kindly copy-paste the URL from below.

To isolate /%(Connection:Client-Mac-Address-NoDelim)/isolate

To unisolate /%(Connection:Client-Mac-Address-NoDelim)/unisolate

**Figure 16: Adding a Context Server Action – Isolate**

![Endpoint Context Server Details](image-url)
Similarly, a Context Server Action to unisolate the endpoint is shown below:

**Figure 17: Adding a Context Server Action – Unisolate**

The next step involves using the above Context Server Action in an Enforcement Profile. The Enforcement Profile to isolate an endpoint leveraging Defender ATP APIs with the defined context server action is shown below.

**Figure 18: Enforcement Profile**

```plaintext
<table>
<thead>
<tr>
<th>Attribute Name</th>
<th>Attribute Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Target Server</td>
<td>172.17.0.2</td>
</tr>
<tr>
<td>2. Action</td>
<td>Defender ATP Isolate</td>
</tr>
</tbody>
</table>
```
The Access Tracker results are shown below. ClearPass Policy Manager triggers an internal API call to the extension configured.

Figure 19: Access Tracker

![Access Tracker](image1)

Extension logs show

Figure 20: Extension Logs

![Extension Logs](image2)
On the client device, it shows:

**Figure 21: Client Device – 1**

![Image showing a message about Internet access being blocked]

**Figure 22: Client Device – 2**

![Image showing a message about network security]

Endpoint can be unisolated using the unisolate action or Enforcement Policy with ClearPass Policy Manager.

Similarly, more context server actions can be configured as shown below:

<table>
<thead>
<tr>
<th>Action Path</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>/macAddress/tag/add/:tagname</code></td>
<td>Adds the specified tag to a device.</td>
</tr>
<tr>
<td><code>/macAddress/isolate</code></td>
<td>Isolates a device.</td>
</tr>
<tr>
<td><code>/macAddress/tag/remove/:tagname</code></td>
<td>Removes the specified tag from a device.</td>
</tr>
<tr>
<td><code>/macAddress/restrictCodeExecution</code></td>
<td>Restrict code execution on a device.</td>
</tr>
<tr>
<td><code>/macAddress/runFullAntiVirusScan</code></td>
<td>Run a Full antivirus scan on a device.</td>
</tr>
<tr>
<td><code>/macAddress/runQuickAntiVirusScan</code></td>
<td>Run a Quick antivirus scan on a device.</td>
</tr>
<tr>
<td><code>/macAddress/unisolate</code></td>
<td>Unisolates a device.</td>
</tr>
<tr>
<td><code>/macAddress/unrestrictCodeExecution</code></td>
<td>Unrestrict code execution on a device.</td>
</tr>
</tbody>
</table>
Microsoft Defender ATP configuration

It is assumed that a working Defender ATP environment is leveraged for this extension. The configuration of defender ATP is beyond the scope of this guide.

To create an app to access Defender ATP, login to Azure portal and navigate to Azure Active Directory > App Registrations > New registration.

Figure 23: create an app to access Microsoft Defender ATP

Follow the steps outlined here: https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/exposed-apis-create-app-webapp

The clientID, clientSecret and tenantID are collected from inside the Defender system. Check out clientSecret is located under Certificates & secrets.

Figure 24: Retrieve clientID, clientSecret, tenantID from Defender ATP
Following permissions are required for all endpoints to work successfully:

**Figure 25: required permissions on Defender ATP**

<table>
<thead>
<tr>
<th>API / Permissions name</th>
<th>Type</th>
<th>Description</th>
<th>Admin Consent Required</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Graph (1)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>User.Read</td>
<td>Delegated</td>
<td>Sign in and read user profile</td>
<td>-</td>
<td>✅ Granted for Aruba, a He,...</td>
</tr>
<tr>
<td>WindowsDefenderATP (15)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AdvancedQuery.ReadAll</td>
<td>Application</td>
<td>Run advanced queries</td>
<td>Yes</td>
<td>✅ Granted for Aruba, a He,...</td>
</tr>
<tr>
<td>Alert.Read.All</td>
<td>Application</td>
<td>Read all alerts</td>
<td>Yes</td>
<td>✅ Granted for Aruba, a He,...</td>
</tr>
<tr>
<td>Ip.Read All</td>
<td>Application</td>
<td>Read IP address profiles</td>
<td>Yes</td>
<td>✅ Granted for Aruba, a He,...</td>
</tr>
<tr>
<td>Machine.Isolate</td>
<td>Application</td>
<td>Isolate machine</td>
<td>Yes</td>
<td>✅ Granted for Aruba, a He,...</td>
</tr>
<tr>
<td>Machine.Read All</td>
<td>Application</td>
<td>Read all machine profiles</td>
<td>Yes</td>
<td>✅ Granted for Aruba, a He,...</td>
</tr>
<tr>
<td>Machine.ReadWrite.All</td>
<td>Application</td>
<td>Read and write all machine information</td>
<td>Yes</td>
<td>✅ Granted for Aruba, a He,...</td>
</tr>
<tr>
<td>Machine.RestrictExecution</td>
<td>Application</td>
<td>Restrict code execution</td>
<td>Yes</td>
<td>✅ Granted for Aruba, a He,...</td>
</tr>
<tr>
<td>Machine.Scan</td>
<td>Application</td>
<td>Scan machine</td>
<td>Yes</td>
<td>✅ Granted for Aruba, a He,...</td>
</tr>
<tr>
<td>Score.ReadAll</td>
<td>Application</td>
<td>Read Threat and Vulnerability Management score</td>
<td>Yes</td>
<td>✅ Granted for Aruba, a He,...</td>
</tr>
<tr>
<td>SecurityConfiguration.Read.All</td>
<td>Application</td>
<td>Read Threat and Vulnerability Management section</td>
<td>Yes</td>
<td>✅ Granted for Aruba, a He,...</td>
</tr>
<tr>
<td>SecurityRecommendation.Read.All</td>
<td>Application</td>
<td>Read Threat and Vulnerability Management section</td>
<td>Yes</td>
<td>✅ Granted for Aruba, a He,...</td>
</tr>
<tr>
<td>Software.Read.All</td>
<td>Application</td>
<td>Read Threat and Vulnerability Management software</td>
<td>Yes</td>
<td>✅ Granted for Aruba, a He,...</td>
</tr>
<tr>
<td>Url.Read.All</td>
<td>Application</td>
<td>Read URL profiles</td>
<td>Yes</td>
<td>✅ Granted for Aruba, a He,...</td>
</tr>
<tr>
<td>User.Read.All</td>
<td>Application</td>
<td>Read user profiles</td>
<td>Yes</td>
<td>✅ Granted for Aruba, a He,...</td>
</tr>
<tr>
<td>Vulnerability.Read.All</td>
<td>Application</td>
<td>Read Threat and Vulnerability Management vulnerability</td>
<td>Yes</td>
<td>✅ Granted for Aruba, a He,...</td>
</tr>
</tbody>
</table>
Appendix A – Additional Diagnostics and Support

The extensions service

The ClearPass extension is supported by a new system service that was initially added in 6.6, but we recommend a minimum version of 6.7.2. 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 ClearPass node] > Service Control. From here start/stop the extension service. By default, this service is automatically started.

Figure 26: Checking on the extensions service and how to start/stop the service

Extension logs and debugging

Referencing the configuration previously used, adjust the logLevel to ‘DEBUG’. In the new 6.7, GUI change the configuration and restart the extension as shown below. Logs can then be viewed from the ‘Show Logs’.

Figure 27: Using the GUI to change the DEBUG level

Remember after changing the logging level, the extension will need to be restarted for this change to take effect.
Monitoring extension statistics

There is a way to monitor extension’s critical statistics with the configurable parameter added as part of the extension’s configuration. To enable extension statistics, make sure to set the “enableStats” parameter to true.

Figure 28: Enable extension statistics

To navigate to statistics page, click Show Details.

Figure 29: Extension Show Details

Open extension statistics URL:

Figure 30: Extension Show Details
This will show
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. The logs are available under Administration > Server Manager > Server Configuration > Collect Logs.

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 that 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. For example, 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 31: Extension logs location in ‘Collect Logs’ diagnostic GZ file