DIGITALIMMUNITY™
STAY PRODUCTIVE, STAY SECURE

Version 3.0

DI PROTECT™

10 February 2020

www.digitalimmunity.com

Copyrights & Trademarks

The contents of this document are the property of Digital Immunity, Inc and are confidential and copyrighted. Use of the Digital Immunity materials is governed by the license agreement accompanying the DI Software. Your right to copy the Digital Immunity Materials and related documentation is limited by copyright law.
Making copies, adaptations, or compilation works (except copies for archival purposes or as an essential step in the utilization of the program in conjunction with the equipment) without prior written authorization from Digital Immunity, Inc is prohibited by law. No distribution of these materials is allowed unless with the explicit written consent of Digital Immunity.

U.S. Government Restricted Rights (Applicable to U.S. Users Only)
Digital Immunity software and documentation is provided with RESTRICTED RIGHTS. The use, duplication, or disclosure by the government is subject to restrictions as set forth in paragraph (c)(l)(ii) of the Rights in Technical Data Computer Software clause at DFARS 252.227-7013. The manufacturer of this Software is Digital Immunity, Inc, 60 Mall Road, Suite 309, Burlington, MA 01803.

Protected by multiple patents. Other patents pending.

DIGITAL IMMUNITY™ is a registered trademark protected by trademark laws under U.S. and international law**.**
All other Intellectual brand and product names are trademarks or registered trademarks of their respective owners.

Product Release: 3.0 (Update 3.0.1)
Last Updated: 10 February 2020

TABLE OF CONTENTS

1 INTRODUCTION

The document communicates the major new features, changes and updates in this release of the DI PROTECT™ v3.0.

2 ABOUT THIS RELEASE

Digital Immunity (DI) keeps its commitment towards ensuring security no longer takes a back seat to production. As a result, we are proud to release DI PROTECT™ v3.0 – the latest and most effective cyber security solution built to keep your Operational Technology and mission critical IT infrastructure productive and secure.

The primary theme of the v3.0 release is *operational efficiency and efficacy*, with DI PROTECT™ receiving important updates and enhancements including:

- Improved management and maintenance of DI Sensors & DI Map Generator(s) through self-updates
- Support for Microsoft Windows XP SP2 operating systems.
- Enhanced protection against Privilege Escalation exploits.
- DI Collector - Centralized multi-site DI PROTECT™ data access.
- DI High Availability – DI PROTECT™ components clustering and operational load balancing.
- Enhanced Countermeasures including
    - Shellcode detection to prevent attackers from remotely gaining control of vulnerable systems.
    - Prevent Byte Code attacks by detecting .NET assemblies being loaded via the CLR (Common Language Runtime)
- Enhanced Threat Hollowing to neutralize Reflective/PE Injection threats, Malicious Script threats and JavaScript Injection attacks
- Numerous other stability updates, fixes and performance enhancements

3 System Requirements

3.1 Operating systems supported

DI Sensor has been tested on the following operating systems:

Server OS

- Microsoft Windows Server 2003 SP2
- Microsoft Windows Server 2008 (including R2)
- Microsoft Windows Server 2012 (including R2)
- Microsoft Windows Server 2016

Workstation OS

- Microsoft Windows XP SP2*new, SP3
- Microsoft Windows Vista
- Microsoft Windows 7
- Microsoft Windows 8
- Microsoft Windows 8.1
- Microsoft Windows 10

3.2 Hardware requirements

Hardware requirements did not change since previous release. For full hardware requirements refer to the ***DI PROTECT™ Administrator Guide***, section ***2.3.1 Hardware/Software Requirements***.

3.3 Other Requirements

3.3.1 Supported Web Browsers

The recommended web-browser to use with DI Control Center is Google Chrome 44.x or later. Other browsers supported are Firefox 45, Internet Explorer 11, Edge 43, Safari 10.8 or higher, but some cross-browser anomalies may exist (refer to section *Known Anomalies* in this document).

3.3.2 Recommended Screen resolution

The recommended resolution for viewing DI Control Center is 1366 x 768. If you use a resolution lower than 1366 x 768, some elements might not be displayed properly on your screen and may impair navigation experience.

4 WHAT'S NEW IN DI PROTECT™ V3.0

4.1 MICROSOFT WINDOWS XP SP2 SUPPORT

DI PROTECT™ is now able to protect endpoints running Microsoft Windows XP SP2.

4.2 DI HIGH AVAILABILITY

The DI High Availability module provides continuous availability of DI PROTECT™ through the clustering of core DI PROTECT™ components. This module offers the following benefits and capabilities:

- ✓ Mitigates single point of failure by allowing distribution of storage management and other DI Map Managers (MMVAs) roles across multiple High Availability cluster nodes.
- ✓ Seamless fully automated fail-over across multiple/stand-by cluster nodes
- ✓ Load balancing and distribution of operational load across multiple DI Map Managers (MMVAs) for optimized performance.
- ✓ Scalable for Enterprise providing the ability to add unlimited nodes in the High Availability cluster.

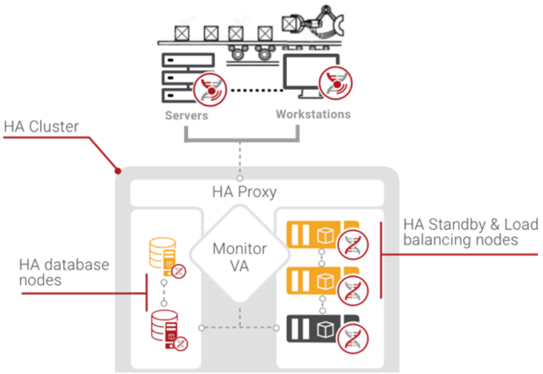
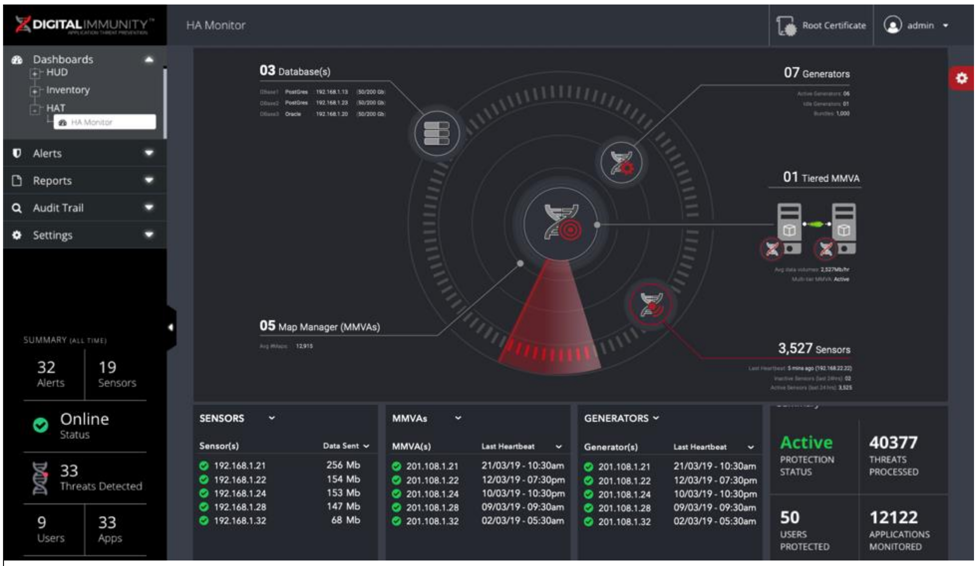


FIGURE 1: ANATOMY OF THE DI HIGH AVAILABILITY CLUSTER

- ✓ Integrates with both local and shared network drives with support for Network File System (NFS), Parallel Network File System (pNFS), Oracle Cluster File System (OCFS2), Amazon Simple Storage Service (S3) and GlusterFS scale-out network-attached storage file systems.
- ✓ Wizard assisted configuration for easy deployment.
- ✓ High Availability Dashboard for operational visibility, see Figure 2



SUMMARY (ALL TIME)

32 Alerts | 19 Sensors

Online Status

33 Threats Detected

9 Users | 33 Apps

SENSORS

Sensor(s)	Data Sent
192.168.1.21	256 Mb
192.168.1.22	154 Mb
192.168.1.24	153 Mb
192.168.1.28	147 Mb
192.168.1.32	68 Mb

MMVAs

MMVA(s)	Last Heartbeat
201.108.1.21	21/03/19 - 10:30am
201.108.1.22	12/03/19 - 07:30pm
201.108.1.24	10/03/19 - 10:30pm
201.108.1.28	09/03/19 - 09:30am
201.108.1.32	02/03/19 - 05:30am

GENERATORS

Generator(s)	Last Heartbeat
201.108.1.21	21/03/19 - 10:30am
201.108.1.22	12/03/19 - 07:30pm
201.108.1.24	10/03/19 - 10:30pm
201.108.1.28	09/03/19 - 09:30am
201.108.1.32	02/03/19 - 05:30am

Active PROTECTION STATUS | 40377 THREATS PROCESSED

50 USERS PROTECTED | 12122 APPLICATIONS MONITORED

FIGURE 2: DI PROTECT™ - HIGH AVAILABILITY DASHBOARD

Refer to the ***DI High Availability Administrator Guide*** for more information.

4.3 DI Collector

The DI Collector provides a single-pane-of-glass view for data collected across multiple sites that are secured by DI PROTECT™. It allows individual sites to send alerts upstream to a central or higher-level DI Collector that would provide a broader view of a large enterprise or global business with multiple business units or departments.

The DI Collector aggregates upstream data sent from existing DI PROTECT™ deployments called 'Sender Sites'. These Sender Sites can be individual DI Map Managers (MMVAs) or part of the DI High Availability clusters located in logical segmentations of the same network, locally distributed sites or geographically remote sites (regional or globally distributed). The Sender site can also be a Collector for other sender sites locally, regionally or globally. See Figure 3.

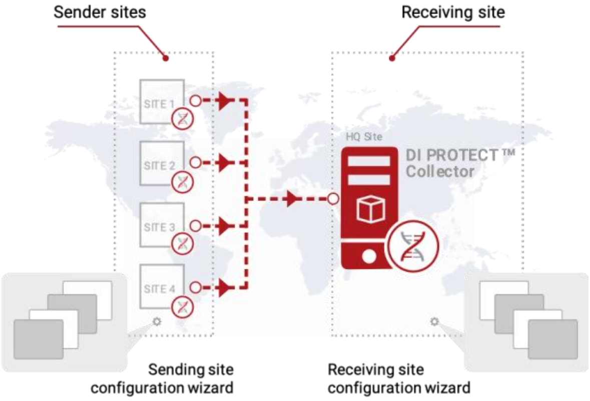
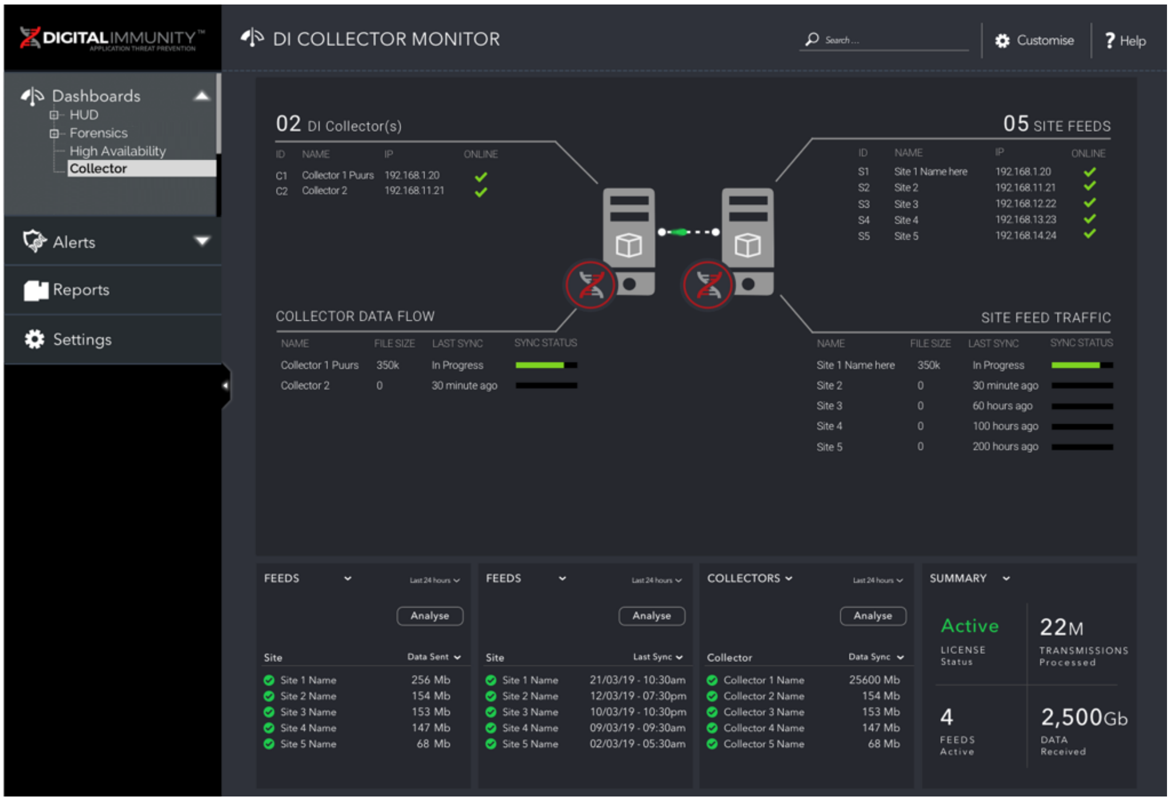


Figure 3: Aggregated data from distributed Sites for a centralized broader view of a large Enterprise



02 DI Collector(s)

ID	NAME	IP	ONLINE
C1	Collector 1 Puurs	192.168.1.20	✓
C2	Collector 2	192.168.11.21	✓

05 SITE FEEDS

ID	NAME	IP	ONLINE
S1	Site 1 Name here	192.168.1.20	✓
S2	Site 2	192.168.11.21	✓
S3	Site 3	192.168.12.22	✓
S4	Site 4	192.168.13.23	✓
S5	Site 5	192.168.14.24	✓

COLLECTOR DATA FLOW

NAME	FILE SIZE	LAST SYNC	SYNC STATUS
Collector 1 Puurs	350k	In Progress	
Collector 2	0	30 minute ago	

SITE FEED TRAFFIC

NAME	FILE SIZE	LAST SYNC	SYNC STATUS
Site 1 Name here	350k	In Progress	
Site 2	0	30 minute ago	
Site 3	0	60 hours ago	
Site 4	0	100 hours ago	
Site 5	0	200 hours ago	

FEEDS — Last 24 hours — Analyse

Site	Data Sent
✓ Site 1 Name	256 Mb
✓ Site 2 Name	154 Mb
✓ Site 3 Name	153 Mb
✓ Site 4 Name	147 Mb
✓ Site 5 Name	68 Mb

FEEDS — Last 24 hours — Analyse

Site	Last Sync
✓ Site 1 Name	21/03/19 - 10:30am
✓ Site 2 Name	12/03/19 - 07:30pm
✓ Site 3 Name	10/03/19 - 10:30pm
✓ Site 4 Name	09/03/19 - 09:30am
✓ Site 5 Name	02/03/19 - 05:30am

COLLECTORS — Last 24 hours — Analyse

Collector	Data Sync
✓ Collector 1 Name	25600 Mb
✓ Collector 2 Name	154 Mb
✓ Collector 3 Name	153 Mb
✓ Collector 4 Name	147 Mb
✓ Collector 5 Name	68 Mb

SUMMARY

Active LICENSE Status	22M TRANSMISSIONS Processed
4 FEEDS Active	2,500Gb DATA Received

Figure 4: DI PROTECT™ Collector Dashboard

The configuration of DI Collector is wizard assisted for easy configuration. For security purposes, each DI Collector can only receive data and cannot write data or change configuration of Sender Sites. See Figure 4.

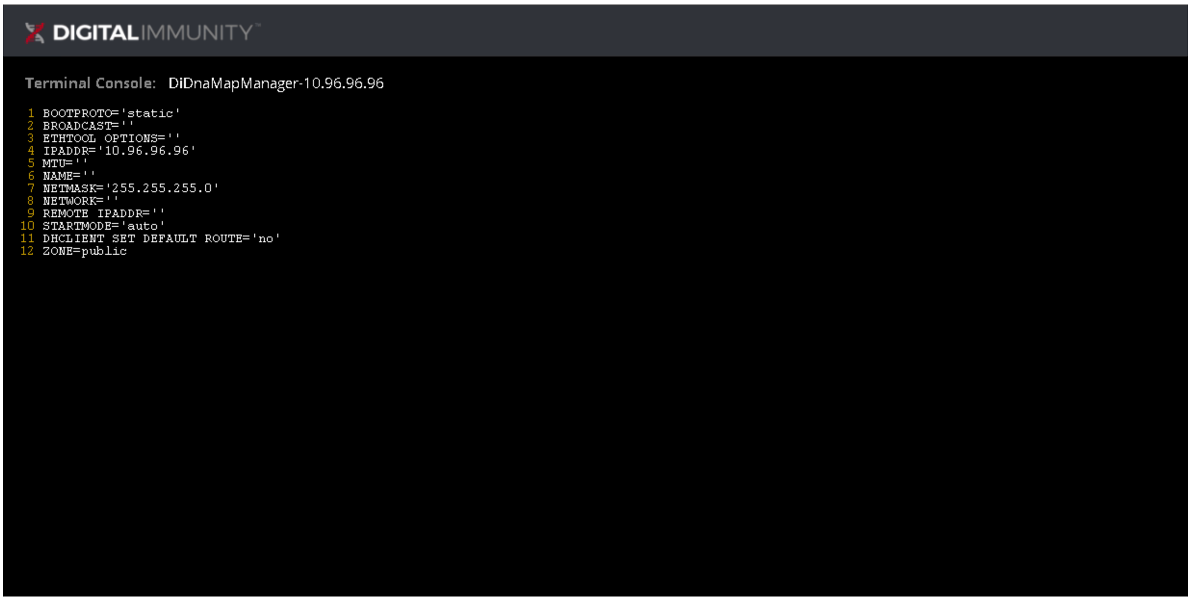
Depending on how your infrastructure is setup, the DI Collector can provide:

- ✓ A centralized view of multiple production lines at large sites
- ✓ A consolidated view of multiple sites – even geographically remote ones.
- ✓ An aggregated view of OT and IT data and activity
- ✓ Full scalability and multi-tiering capabilities regardless of network segmentation or physical location of the site.
- ✓ Forwarding of alerts through a DMZ

Refer to the ***DI Collector Administrator Guide*** for more information.

4.4 Virtual Console

DI PROTECT™ v3.0 includes a Terminal (Virtual) Console. This provides a command-line interface for administrators to open a terminal session and execute command-line instructions on DI Map Manager(s), including the ones in a DI High Availability cluster setup. See Figure 5.



Terminal Console: DiDnaMapManager-10.96.96.96

```
BOOTPROTO='static'
BROADCAST=''
ETHTOOL OPTIONS=''
IPADDR='10.96.96.96'
MTU=''
NAME=''
NETMASK='255.255.255.0'
NETWORK=''
REMOTE IPADDR=''
STARTMODE='auto'
DHCLIENT SET DEFAULT ROUTE='no'
ZONE=public
```

Figure 5: DI PROTECT™ - Virtual Console

4.5 Enhanced Features

4.5.1 Enhanced Shellcode Detection

The countermeasures of DI PROTECT™ v3.0 have been enhanced through the addition of new Shellcode properties for deeper protection against command shell exploits. Malicious shellcodes are segments of binary code disguised as normal input data. These can be injected at runtime to overwrite legitimate processes and hijack control flow.
The new Shellcode properties in DI PROTECT™ v3.0 enable optimized detection and filtering of malicious shellcode to prevent damage and harden operating systems and related applications against exploits that enable attackers to hijack endpoints.

4.5.2 Enhanced Threat Hollowing countermeasure

For specific alert types and threats, DI PROTECT™ can also neutralize (render inert/core-out) specifically the malicious part of a process while keeping the legitimate parts of the same process running without interference or disruption. This feature is known as Threat Hollowing and prior to DI PROTECT™ v3.0, this countermeasure could be applied against these specific threats:

- Heap Code Execution attacks
- Unauthorized Functions threats
- Malicious Shellcode attacks

In DI PROTECT™ v3.0, we have extended Threat Hollowing capabilities to also neutralize malicious processes related to the following threats – without interfering with the legitimate parts of an infected application process:

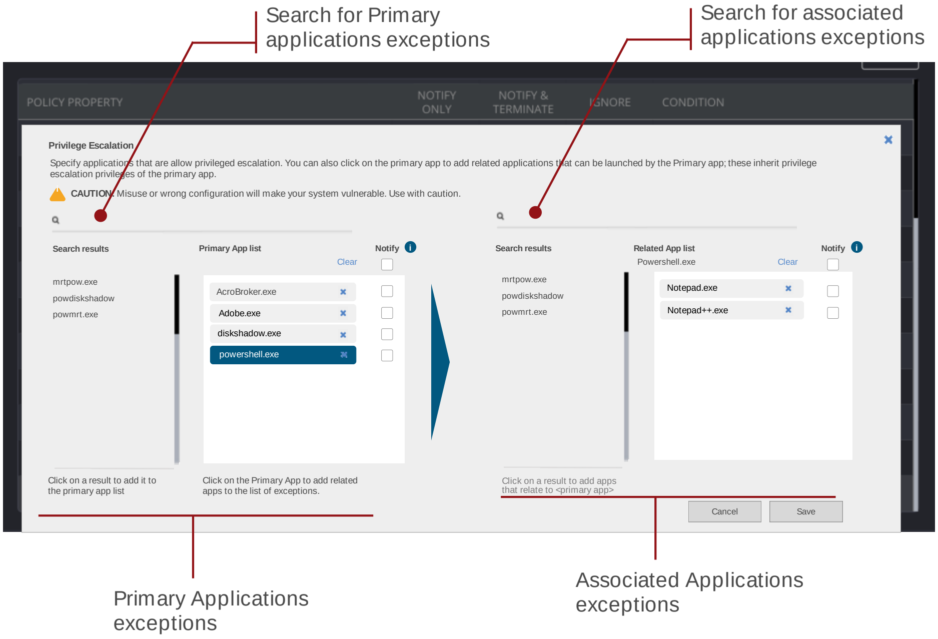
- Reflective/PE Injection threats
- Malicious Script threats
- JavaScript Injection attacks

4.5.3 Added countermeasures against Byte Code attacks

DI PROTECT™ v3.0 includes new countermeasures which protect against Byte Code attacks. In this version, DI PROTECT™ is now able to detect and prevent Virtual Machine escape vulnerabilities that may be exploited using .NET assemblies loaded via the CLR (Common Language Runtime) to compromise hosts.

4.5.4 Enhanced control over privilege escalation threats & Exceptions

In the previous version of DI PROTECT™, privilege escalation exceptions could be set only on individual applications. While this is good, certain applications such as command processors (e.g. cmd.exe or powershell.exe) can invoke other legitimate binaries or processes for which an exception is not set. As of DI PROTECT™ v3.0, administrators can also associate other processes and binaries to an application in the exception list.



Privilege Escalation

Specify applications that are allow privileged escalation. You can also click on the primary app to add related applications that can be launched by the Primary app; these inherit privilege escalation privileges of the primary app.

CAUTION: Misuse or wrong configuration will make your system vulnerable. Use with caution.

Click on a result to add it to the primary app list

Click on the Primary App to add related apps to the list of exceptions.

Click on a result to add apps that relate to <primary app>

Figure 6: DI PROTECT™ Enhanced Privilege Escalation exceptions

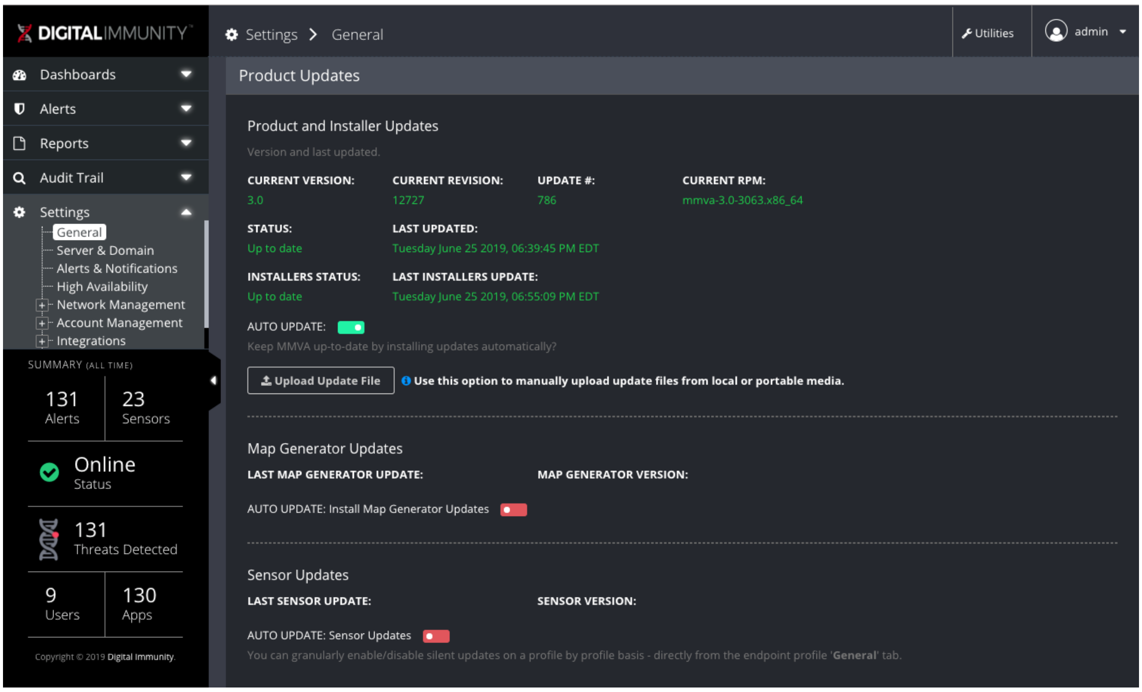
The privilege escalation exception will apply only when the associated binaries are invoked by the primary application(s). This means that if other applications (e.g. not authorized applications) invoke these same binaries, the exception rule will not be applied.
Privilege escalation exception rules in DI PROTECT™ only apply when the combined rule criteria *<primary app><associated binaries>* (e.g. cmd.exe > notepad++.exe) as configured by the administrator is met/matched in full. This allows more control when setting up privilege escalation exceptions without compromising protection. See Figure 6.

Example: cmd.exe > notepad++.exe

If *cmd.exe* is allowed privilege escalation as a primary app, and *notepad++.exe* is configured as an associated application, privilege escalation exception for *notepad++.exe* is ONLY allowed when this is invoked/opened via *cmd.exe.*
In this same case, if *notepad++.exe* is invoked using another method like PowerShell scripts, the privilege escalation exception is NOT ALLOWED. To allow this, the administrators need to add also *Powershell.exe* to the primary app exceptions and associate *notepad++.exe* with it.

4.5.5 DI Sensor & DI Map Generator Self Updates

DI PROTECT™ now allows administrators to enable self-updates on DI Sensors and DI Map Generators. This functionality can now be enabled from the DI PROTECT™ Control Center. See figure 7.



Product Updates

Product and Installer Updates

Version and last updated.

CURRENT VERSION: 3.0
CURRENT REVISION: 12727
UPDATE #: 786
CURRENT RPM: mmva-3.0-3063.x86_64

STATUS: Up to date
LAST UPDATED: Tuesday June 25 2019, 06:39:45 PM EDT

INSTALLERS STATUS: Up to date
LAST INSTALLERS UPDATE: Tuesday June 25 2019, 06:55:09 PM EDT

AUTO UPDATE: 🟩

Keep MMVA up-to-date by installing updates automatically?

Upload Update File — Use this option to manually upload update files from local or portable media.

Map Generator Updates

LAST MAP GENERATOR UPDATE:
MAP GENERATOR VERSION:

AUTO UPDATE: Install Map Generator Updates 🟥

Sensor Updates

LAST SENSOR UPDATE:
SENSOR VERSION:

AUTO UPDATE: Sensor Updates 🟥

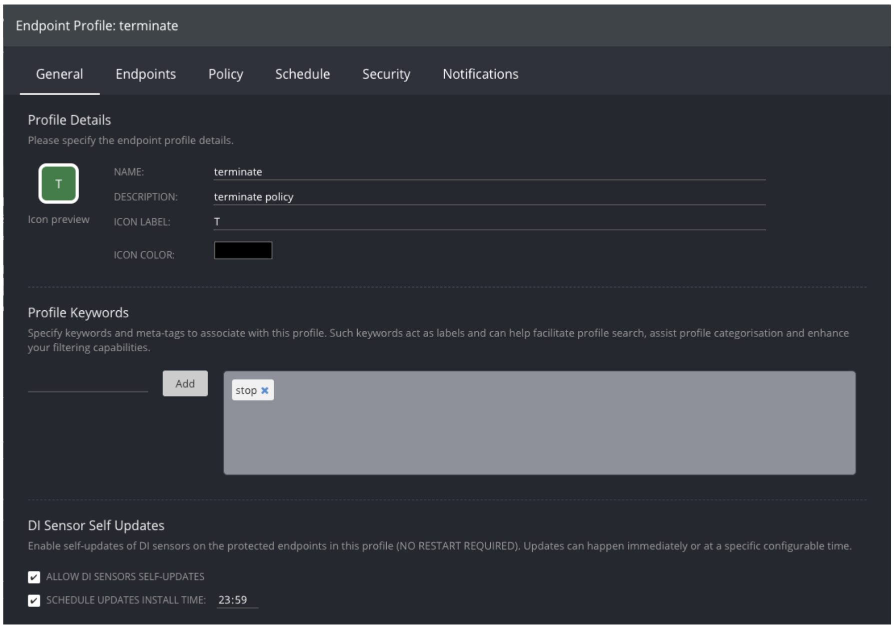
You can granularly enable/disable silent updates on a profile by profile basis - directly from the endpoint profile '**General**' tab.

Figure 7: Self-Update Settings for DI Sensors & DI Map Generators

When DI Sensors and/or DI Map Generators identify a new update, they can:

- Automatically and safely unload DI Sensor or DI Map Generator accordingly
- Automatically install updates and re-launch the DI Sensor and/or DI Map Generator

All this is done seamlessly and without disruption to your productivity. The self-update feature can be enabled and configured via DI Control Center; for DI Sensors, administrator can also granularly enable DI Sensor self-updates on a subset of endpoints via the Endpoint Profile. This granular configuration of Self Updates from Endpoint Profile also allows for the scheduling of updates at a specific time to align with your organizational maintenance schedules and requirements.



Endpoint Profile: terminate

Profile Details

Please specify the endpoint profile details.

Icon preview: T

NAME: terminate
DESCRIPTION: terminate policy
ICON LABEL: T
ICON COLOR: ■

Profile Keywords

Specify keywords and meta-tags to associate with this profile. Such keywords act as labels and can help facilitate profile search, assist profile categorisation and enhance your filtering capabilities.

stop ✖

DI Sensor Self Updates

Enable self-updates of DI sensors on the protected endpoints in this profile (NO RESTART REQUIRED). Updates can happen immediately or at a specific configurable time.

☑ ALLOW DI SENSORS SELF-UPDATES
☑ SCHEDULE UPDATES INSTALL TIME: 23:59

Figure 8: Granular Self-Updates settings from Endpoint Profile

4.5.6 ADDITIONAL MINOR ENHANCEMENTS

- In the Audit Trail log, hyperlinks are added to forensics page to access further details where applicable. This enhances the navigation experience when analyzing audit trail logs.
- Added failover support for database and web interfaces.
- Automatically create application groups from map entries for enhanced performance and better application management/data presentation.
- Automatically create application groups for unauthorized applications for enhanced performance and better application management/data presentation.
- Optimize performance through the separation of database server functions from DI Map Manager.
- Migrated DI Map Manager code base to Python 3.
- Migrated Django framework to latest version for increased stability and compatibility.
- Upgrade Secure boot protection for increased protection against unsigned and malicious boot loaders.
- Optimize DI Generator Tuning for increased stability and performance.

DIGITAL IMMUNITY™
STAY PRODUCTIVE, STAY SECURE

Digital Immunity
60 Mall Road
Suite 309
Burlington, MA 01803
(781) 425-8655

Sales Inquiries:
Sales@digitalimmunity.com

General Inquiries:
Info@digitalimmunity.com