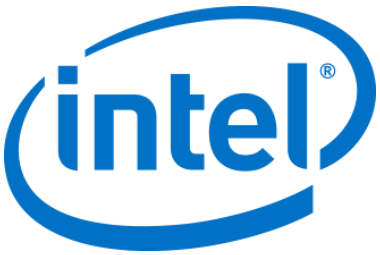


Intel® Accelerated Storage Manager Release 2.0

Windows* Administration Guide

April 2019
Revision 2.0

Document Number: 338849-002US

Revision History

Revision Number	Description	Revision Date
0.1	Initial version	June 2016
1.0	Full Release	March 2017
1.1	Update to 1.1 release	April 2017
1.2	Update to 1.2 release	June 2017
1.3	Update to 1.3 release	September 2017
1.4	Update to 1.4 release	February 2018
2.0	Update to 2.0 release	April 2019

Contents

1 Introduction

1.1 Purpose and Scope of this Document

This document offers the guidance to learn, install and use Intel® Accelerated Storage Manager.

This guide assumes a basic knowledge of storage, application, services management and Microsoft* Windows* Operating System.

1.2 Acronyms and Definitions

Table 1: Terminology

Term	Definition
HTTP/HTTPS	Hyper Text Transport Protocol, application protocol that is a base standard used in WWW.
Certificate Authority	Trusted entity used to sign digital certificates.
HTTPS Certificate	Digital certificate used in data encryption.
REST	Representational State Transfer, a software architecture approach for building scalable web services.
JSON	JavaScript Object Notation, a human readable format used to transmit data.
URI	Unified Resource Identification standard, a string and number standard used to uniquely identifying resource in i.e. network.
OAuth 2.0	Three-legged token based authentication protocol used commonly in REST APIs.
OAuth 2.0 Grant	Method of authentication used by OAuth 2.0.
OAuth 2.0 Scope	Name of the part of protected resource.
Static Content	Web application or HTML/JavaScript/CSS pages that can be hosted from web server.
SSD	Solid State Drive. A device used for data storage that uses non-volatile memory chips instead of a rotation disk.
S.M.A.R.T	Self-Monitoring, Analysis and Reporting Technology, monitoring system included in HDD/SSD disks that reports various drive information.
RAID	Redundant Array of Independent Disks.
VROC	Intel® Virtual RAID on CPU.

§

2 Product Overview

2.1 Intel® Accelerated Storage Manager

The Intel® Accelerated Storage Manager (Intel® ASM) project aims to provide REST API capabilities for various, supported Intel storage products.

Intel® ASM is complete RESTful solution providing, among others, features like REST API for system and devices information, RAID information through VROC plugin, authentication and authorization using OAuth 2.0, web page and application serving through built-in web server.

2.2 System Requirements

Table 2: System Requirements

Platform	Architecture
Microsoft Windows* 10	x64
Microsoft Windows* Server 2012 R2 Enterprise	x64
Microsoft Windows* 8.1	x64
Microsoft Windows* 7 SP1	x64
Microsoft Windows* Server 2016 Enterprise	x64

§

3 Quick Installation Guide

This section is focused to show how to correctly configure Intel ASM to work on localhost (on the same machine) and login as Administrator. More detailed steps are in next sections.

1. Install INTEL ASM using default options in the installer.
2. In the Windows Explorer, go to:
   C:\Program Files\Intel\Intel Accelerated Storage Manager
3. Open iasm.conf with Notepad or anything suitable to edit plain text (click it with RMB and then choose Open with...)
4. Go to the very bottom of the file.
5. For each [scope], remove '#' character before "groups" and add "Administrators" (without quotation marks) after '='. Case insensitive.
6. Safe the file.
7. RMB on Start -> Run (Win + R), write "services.msc" (without quotation marks) and press Enter.
8. Find Intel® Accelerated Storage Manager Service.
9. RMB on it and choose "Restart".
10. Wait till INTEL ASM restarts successfully. If INTEL ASM status is not "Running", configuration file has format errors.
11. Open browser and just type in url field: localhost
    Browser should open page named: localhost/#/login
12. Login as Administrator using Windows password. Leave "domain" empty.

§

4 Theory of Operation

4.1 Service Operation Modes

Depending on configuration, Intel ASM can work in several operating modes.

One instance of Service can operate in one or many modes at a time.

Following sections describe available modes in detail.

4.1.1 Authentication Server

This is a mandatory mode to be used with Intel ASM. Depending on configuration at least one authentication server needs to be present in the network in order to provide user authentication and authorization.

Intel ASM Service, configured to act as such server, provides OAuth 2.0 interface for client applications. To perform authentication, service can be configured to use OS user database or domain database.

Each application, before using REST API, needs to authenticate itself to this server to obtain special access token, used later in client – server communication.

For details about using authentication mechanism refer to Intel ASM Security API specification.

4.1.2 Resource Server

Resource server is a basic mode of Intel ASM. It provides REST API capabilities listed below:

- **System Information**: basic information about platform and system where server is running, such as name and version of the running operating system, CPU and Memory usage as well as performance information.
- **SSD Information**: set of information about connected SSD devices and partial information about HDD devices, like device identity and S.M.A.R.T.
- **VROC Management:** provides management capabilities for Intel® Virtual RAID on CPU.

For more details about REST APIs, refer to Intel ASM REST specifications (Section **Error! Reference source not found.**).

4.1.3 Application Server

One of the features of Intel Accelerated Storage Manager is to serve static content (HTML pages or HTML/JavaScript applications).

After configuring Intel ASM, such application will be available on given IP address and port.

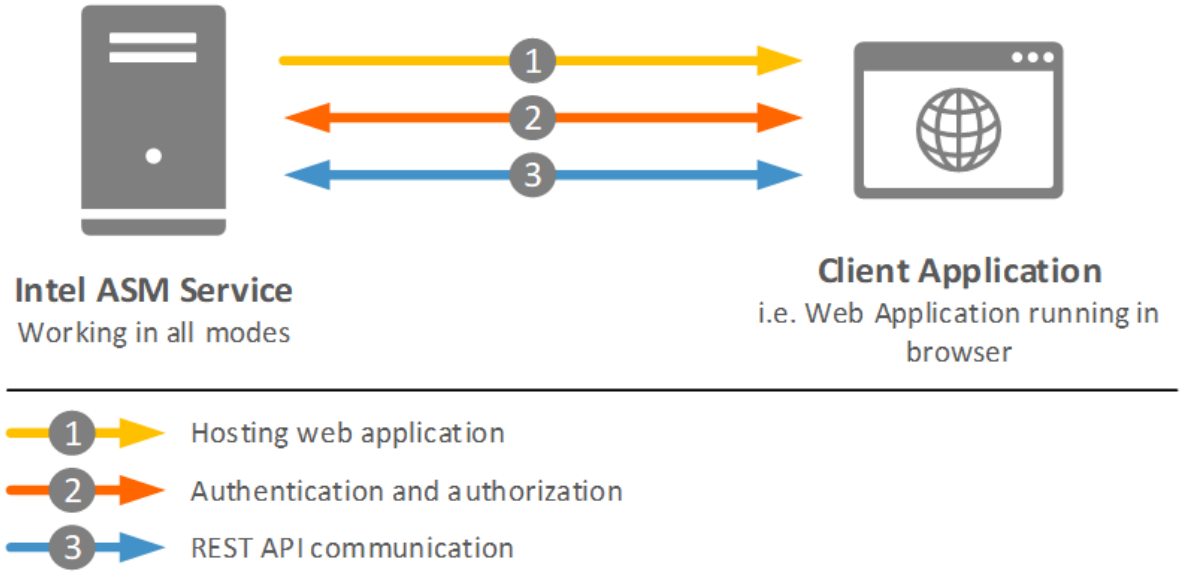
However, Intel ASM is not responsible for application functioning except the Intel ASM Management Console provided with this release.

4.2 Standalone Configuration

Depending on user choice, Intel Accelerated Storage Manager can be configured to run on one server machine – in standalone configuration.

In such configuration, service runs in all operation modes at a time. It provides authentication interface, application server and resource server capabilities on a single machine, under one configured IP address and port (see Figure 1).

Figure 1: Intel® ASM Standalone Configuration



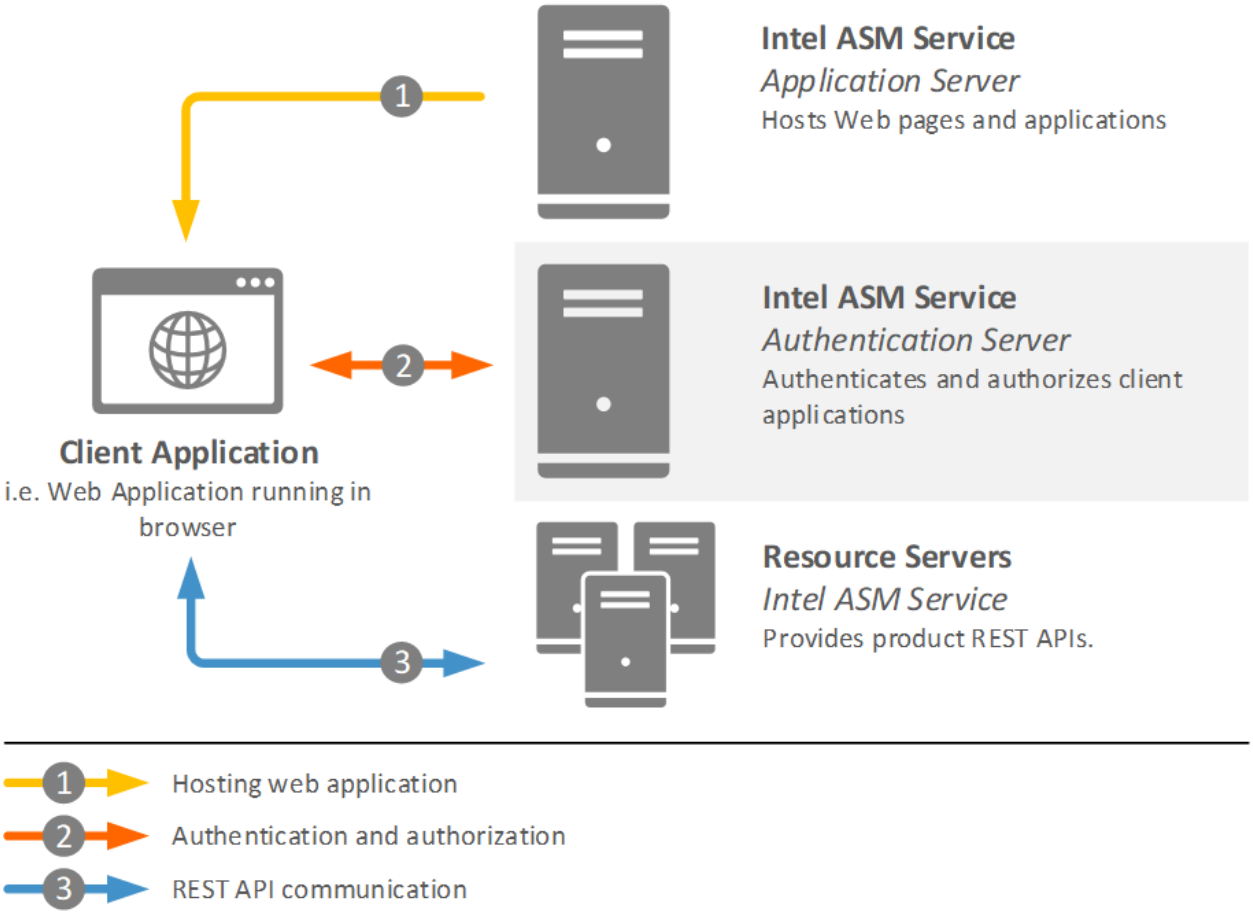
4.3 Distributed Configuration

If usage of multiple server machines is planned, Intel ASM shall be configured in distributed configuration. This configuration allows to use one authentication end-point and one application server to manage resource servers (see Figure 2).

Web application i.e. Intel ASM Management Console can be hosted from one dedicated machine. To perform authentication, client application running in web browser will then use one, known authentication server, instead of authenticating with each resource server separately.

After successful sign in, client application can communicate with selected resource server using REST API.

Figure 2: Intel® ASM Distributed Configuration



§

5 Getting Started

5.1 Package Contents

For all supported systems, Intel Accelerated Storage Manager is released as installation packages.

For Windows* family systems package is in a form of one installation executable included in VROC 6.0 installer.

Intel Accelerated Storage Manager package contains:

- HTTP Service core binaries and configuration file.
- VROC Plugin to manage the product.
- System Plugin providing information about basic platform configuration.
- SSD Plugin providing device specific information.
- Web management console, a WEB GUI application to manage products through REST API.

5.2 System Preparation

If usage of HTTPS is planned (which is strongly recommended for security reasons), Network or System Administrators or any authorized entity should create, sign and configure proper HTTPS certificates. For details of this configuration see Section **Error! Reference source not found.**.

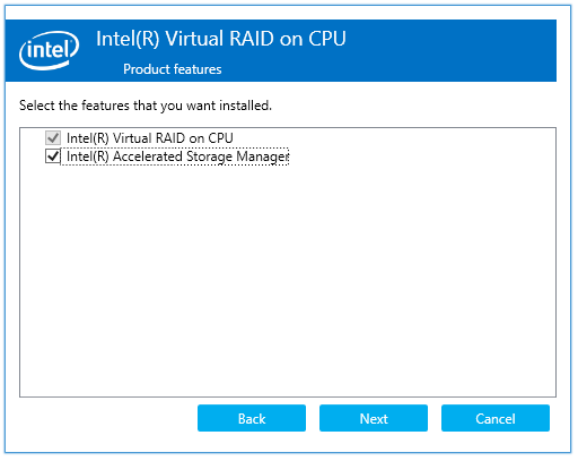
Note: Intel recommends installing and configuring Intel ASM only in local trusted network. Intel is not responsible for any damage caused by enabling remote access from public networks/Internet.

Windows* Installer for Intel Accelerated Storage Manager already contains all necessary prerequisites, there are no additional requirements to configure the system itself.

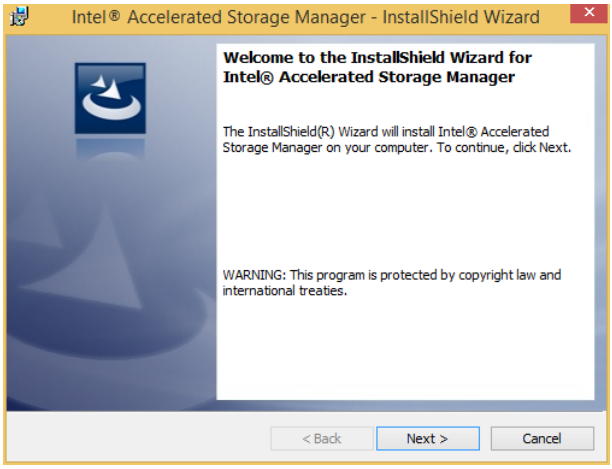
5.3 Installing Intel® ASM

5.3.1 Using Windows* Installer

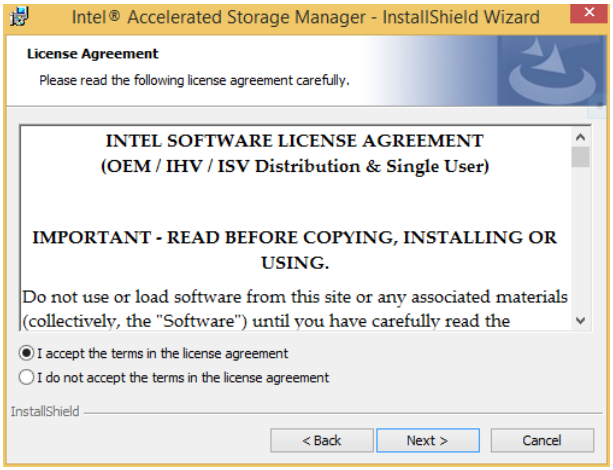
This version of Intel Accelerated Storage Manager is installed along with VROC 6.0 product. All files and components are included in this installation package.



In order to properly install Intel® ASM a checkbox with “Install Intel® Accelerated Store Manager” should be in VROC 6.0 installer.

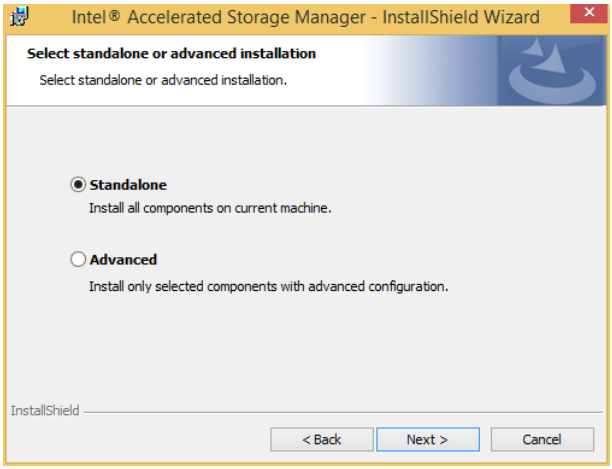


VROC 6.0 installer will then automatically launch installation of Intel Accelerated Storage Manager.



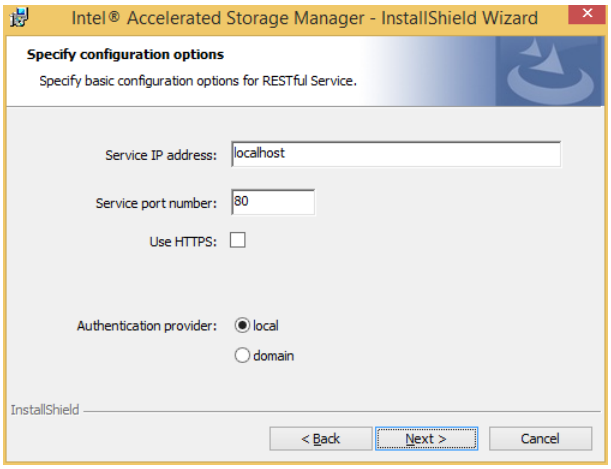
In the next step installer will display license agreement.

In order to proceed user must read and accept terms of this license.



Installer provides two types of installation:

- A “Standalone” version where installer installs all components in a default configuration on current machine.
- An “Advanced” version where user can choose components which will be installed and installer allows to configure product in advanced mode then.

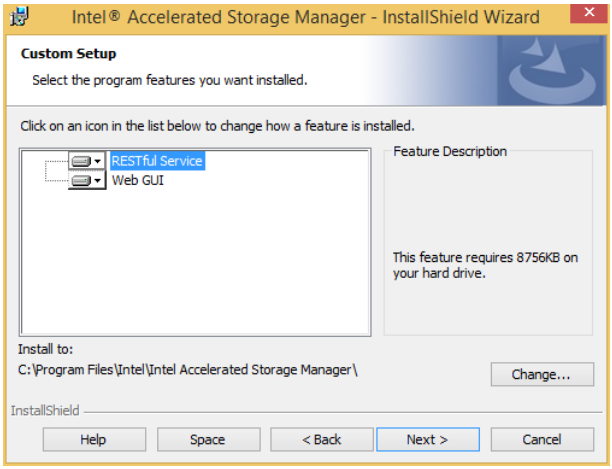


In basic configuration user can configure following options:

- Service IP address,
- Service port number,
- Authentication provider.

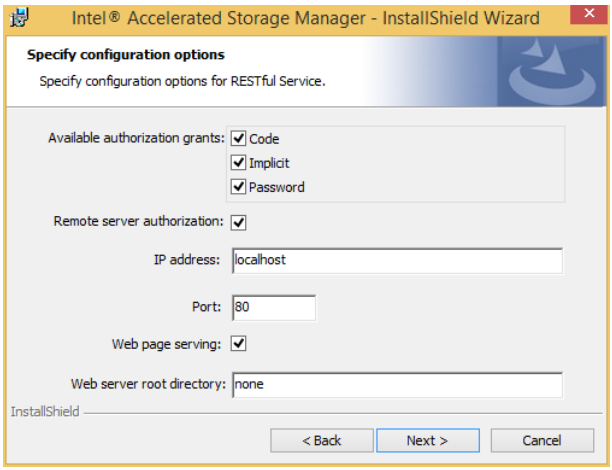
Also HTTPS option can be selected. In such case path to HTTPS certificate must be given.

Above configuration options are also available in advanced mode.



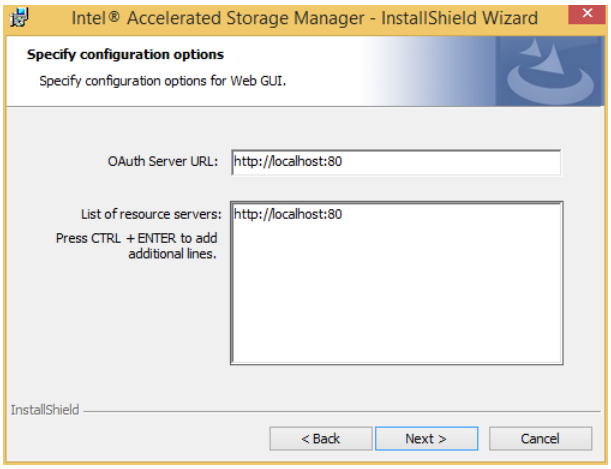
Advanced installation provides additional wizard screens and options.

It allows to choose which components are installed and to change the destination path.



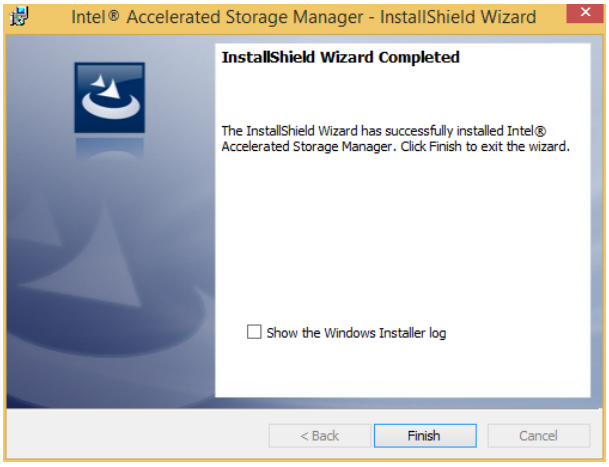
Additional HTTP service options can be set, such as:

- Available OAuth 2.0 authorization grants.
- Remote server authorization parameters.
- Web page serving with web server root directory path.



Advanced installation allows also to set Web Management Console options like:

- OAuth 2.0 Authentication server URI.
- URIs of Intel Accelerated Storage Manager instances working in resource server operating mode.



Regardless of chosen installation type installer informs user about completion status.
For troubleshooting, installer log can be inspected.

5.3.2 Using Windows* Installer from Command Line

Intel Accelerated Storage Manager can be installed in silent mode using command line parameter.

Usage:

```
SetupVROC.exe -s -IASM_INSTALL_IN_SILENT [-IASM_HOST]
[-IASM_PORT] [-IASM_HTTPS] [-IASM_CERTIFICATE]
[-IASM_OA_AUTH_PROVIDER] [-IASM_OA_GRANTS] [-IASM_OA_SERVER]
[-IASM_OA_SERVER_HOST] [-IASM_OA_SERVER_PORT]
[-IASM_WEB_SERVER_INSTALL] [-IASM_WEB_SERVER] [-IASM_WEB_CONTENT]
[-IASM_AUTHORIZATION_URL] [-IASM_AGENT_URL_ARRAY]
```

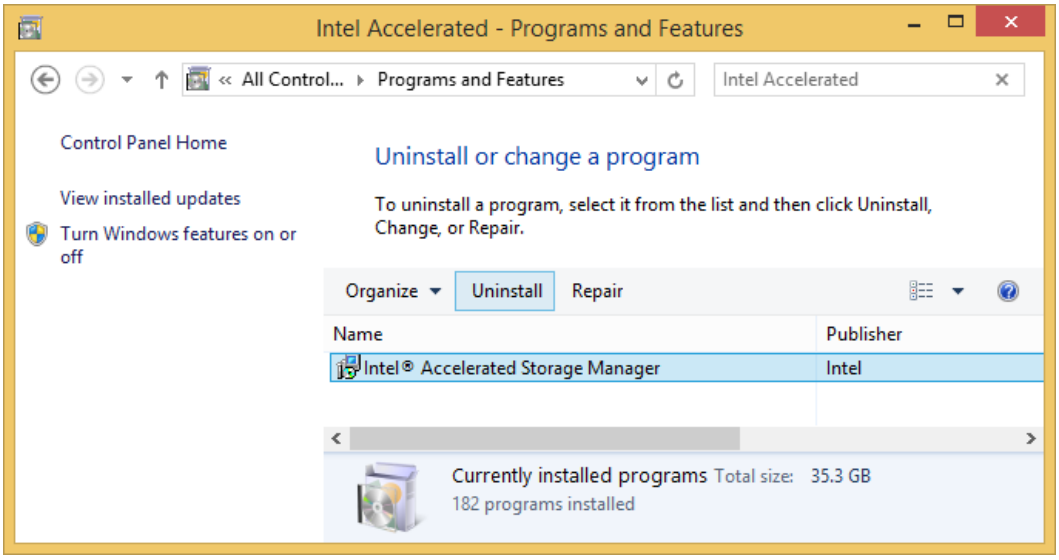
Options:

Config Parameter	Option	Description
Required parameter	-s	Installer in silent mode
Required parameter	- IASM_INSTALL_IN_SILENT	Install IASM
host	-IASM_HOST	HTTP Server IP address
port	-IASM_PORT	HTTP Server port
https	-IASM_HTTPS	Set https on or off. (true/false)
Certificate	-IASM_CERTIFICATE	Path to certificate, if https is on. Set "none" or "non" if no path was specified.
oa_auth_provider	-IASM_OA_AUTH_PROVIDER	Set authentication provider. (local/domain)
Installation parameter	-IASM_WEB_SERVER_INSTALL	Web server GUI installation. (true/false)
web_content	-IASM_WEB_CONTENT	Path to directory with webpage files. Set "none" or "non" if no path was specified.
web_server	-IASM_WEB_SERVER	Enables webpage serving. (true/false)
oa_server	-IASM_OA_SERVER	Enable authorization on remote server. (true/false)
oa_server_host	-IASM_OS_SERVER_HOST	Authorization server IP address
oa_server_port	-IASM_ OA_SERVER_PORT	Authorization server port
oa_grants	-IASM_OA_GRANTS	Set grants supported by authorization server. (code,implicit,password)
authorization_url	-IASM_ AUTHORIZATION_URL	OAuth2.0 URL using by GUI to authorization
agent_url	-IASM_AGENT_URL	Server URL with RESTful Service (URL)

5.4 Uninstalling Intel® ASM

To uninstall this product, administrator should navigate to Control Panel → Program and Features, select Intel Accelerated Storage Manager and click "Uninstall" button (Figure3).

Figure 3: Uninstalling Intel Accelerated Storage Manager



§

6 Configuring Intel® ASM

6.1 HTTPS Recommended Configuration

For security reasons, it is highly recommended to use HTTPS communication. Unencrypted communication can lead to security vulnerability and cause, among other concerns, leak of sensitive data.

Intel Accelerated Storage Manager can use valid and signed digital certificates to communicate over HTTPS.

To use HTTPS users need to be able to generate and sign such certificates. Certificate generation can be done on any machine with proper tools, however signing requires specific network and services configuration.

To sign certificate in local network at least one trusted Certificate Authority (CA) needs to be available and CAs root certificate needs to be propagated to all client machines.

Configuration of such environment is beyond the scope of this guide.

6.1.1 HTTPS Configuration Policies

6.1.1.1 Private Key Strength

Keys should be strong and remain strong for the planned lifetime. For use in Intel Accelerated Storage Manager Service, at least **2048** bit private key is recommended.

6.1.1.2 Private Key and Certificate Protection

Keys are very important and sensitive assets. They need to be stored in a secure location, under an access control, like file system with Access Control List on a trusted computer.

Always limit access only to minimum number of users.

If the key is compromised, it is always necessary to create a new key and revoke existing certificates.

It is highly recommended to renew certificates at least once in a year, with new private key.

6.1.1.3 Certification Authority (CA)

All used certificates should be signed by trusted Certification Authority. It is not recommended to use self-signed certificates.

Certification Authority shall be reliable, known and trusted, however it is up to network Administrators or other authorized entity to choose CA, since it is specific and dependent on current network infrastructure.

6.1.1.4 Certificate Chain of Trust

Always provide all intermediate certificates to ensure that path validation is done correctly on client side.

6.1.2 HTTPS Configuration

The following sections describes sample generation of key and certificate signing request. All below examples use OpenSSL toolkit and assume that OpenSSL is already installed on configured machine

6.1.2.1 Generating Private Key

Before generating signed request, private key needs to be created. Following example generates 2048 bit RSA key.

```
$ openssl genrsa -out ~/private.key 2048
Generating RSA private key, 2048 bit long modulus
.....................+++
.................................+++
e is 65537 (0x10001)
```

6.1.2.2 Generating Certificate Signing Request (CSR)

Command below generates CSR with use of private key. In this process, user will need to enter additional information. Using sha256 here is highly recommended.

```
$ openssl req -new -sha256 -key ~/private.key -out request.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:PL
State or Province Name (full name) [Some-State]:Pomerianian
Locality Name (eg, city) []:Gdansk
Organization Name (eg, company) [Internet Widgits Pty Ltd]:My Corporation
Organizational Unit Name (eg, section) []:MyUnit
Common Name (e.g. server FQDN or YOUR name) []:restapi.mycorp.com
Email Address []:johndoe@mycorp.org

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

The following command can be used to validate created CSR:

```
$ openssl req -noout -text -in ~/request.csr
Certificate Request:
    Data:
        Version: 0 (0x0)
        Subject: C=PL, ST=Pomerianian, L=Gdansk, O=My Corporation, OU=MyUnit, CN=
restapi.mycorp.com /emailAddress= johndoe@mycorp.org
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:d6:c9 ...
                Exponent: 65537 (0x10001)
        Attributes:
            a0:00
    Signature Algorithm: sha256WithRSAEncryption
         69:bc:2e ...
```

6.1.2.3 Submitting CSR

Generated CSR should be now submitted to CA in order to be signed. Certificate Authority, if CSR will be issued successfully, will return signed certificate.

Form and process of submission and signing depends on CA policies.

Since configuration of Certificate Authority and issuing process is different depending on used technology and infrastructure setup, signing process will not be described in this document.

6.1.2.4 Using Signed Certificate in HTTP Service

Intel Accelerated storage manager uses private key and certificate stored in one file. Use following command to create such file (assuming that signed certificate returned by CA is named "signed.pem"):

```
(openssl x509 -in signed.pem; cat private.key) > iasm.pem
```

In order to use signed certificate, Administrator must set following options in the configuration file and restart Intel ASM service:

```
…
port = 443
https = true
certificate = /path-to-certificate-directory/iasm.pem
…
```

6.2 Command Line Configuration

Preferred configuration method of Intel Accelerated Storage Manager is to run service executable with proper command line options. This method will not only write provided options to file, but it will also validate configuration file correctness.

To print all available commands with parameters run service executable with "help" command.

6.2.1 Command Line Options

6.2.1.1 “serve” Command

Usage:

```
iasm serve [-I][--host] [-P][--port] [-H][--https]
[-C][--certificate] [-X][--http-threads] [-Y][--plug-threads]
[-Z][--plug-timeout] [-V][--oa-auth-provider] [-D][--web-content]  [-S][--web-server]
[-A][--oa-server] [-O][--oa-server-host]
[-T][--oa-server-port] [-B][--oa-token-expiration-time]
[-E] [--oa-code-expiration-time] [-R][--oa-refresh-expiration-time]  [-
G][--oa-grants]
```

Options:

Config Parameter	Option	Short Option	Description
host	--host	-I	HTTP Server IP address (127.0.0.1 for local offline configuration)
port	--port	-P	HTTP Server port
https	--https	-H	Set http on or off. (true/false)
certificate	--certificate	-C	Path to certificate, if https is on. Set "none" or "non" if no path was specified.
http_threads	--http-threads	-X	Set number of threads handling requests in HTTP server
plugins_threads	--plug-threads	-Y	Set number of threads handling request's code execution in plugins
plugins_timeout	--plug-timeout	-Z	Set timeout on request's code execution in plugin
oa_auth_provider	--oa-auth-provider	-V	Set authentication provider. (local/domain)
web_content	--web-content	-D	Path to directory with webpage files. Set "none" or "non" if no path was specified.
web_server	--web-server	-S	Enables webpage serving. (true/false)
oa_server	--oa-server	-A	Enable authorization on remote server. (true/false)
oa_server_host	--oa-server-host	-O	Authorization server IP address
oa_server_port	--oa-server-port	-T	Authorization server port
oa_token_expiration_time	--oa-token-expiration-time	-B	Set access token expiration time. (in seconds)
oa_code_expiration_time	--oa-code-expiration	-E	Set access code expiration time. (in seconds)
oa_refresh_expiration_time	--oa-refresh-expiration	-R	Set refresh token expiration time. (in seconds)
oa_grants	--oa-grants	-G	Set grants supported by authorization server. (code,implicit,password)

6.2.1.2 Client Applications Management

6.2.1.2.1 New Client Registration

Usage:

```
iasm register_client [-C][--client_id] [-S][--scopes] [-G][--grants]
```

Options:

Config Parameter	Option	Short Option	Description
client_id	--client_id	-C	ID of client to be added
scopes	-scopes	-S	Scopes to which client will have an access separated by comma. Scope format: ip@scope. No ip defines scope for all resource servers
grants	--grants	-G	Grants allowed to use by new client separated by comma (implicit,code)

6.2.1.2.2 Unregistering Client Application

Usage:

```
iasm remove_client [-C][--client_id]
```

Options:

Config Parameter	Option	Short Option	Description
client_id	--client_id	-C	ID of client to remove

6.2.1.2.3 Updating Client Information

If key is left empty, its value will be erased.

Usage:

```
iasm update_client [-C][--client_id] [-S][--scopes] [-G][--grants]
```

Options:

Config Parameter	Option	Short Option	Description
client_id	--client_id	-C	ID of client to be added
scopes	-scopes	-S	Scopes to which client will have an access separated by comma. Scope format: ip@scope. No ip defines scope for all resource servers
grants	--grants	-G	Grants allowed to use by new client separated by comma (implicit,code)

6.2.1.3 Scopes Management

6.2.1.3.1 Adding New Scope

Usage:

```
iasm add_scope [-N][--name] [-U][--users] [-G][--groups]
```

Options:

Config Parameter	Option	Short Option	Description
name	--name	-N	Name of scope to be added with ip address of resource server. Format: ip@scope. No ip defines scope for all resource servers.
scopes	-scopes	-S	Scopes to which client will have an access separated by comma. Scope format: ip@scope. No ip defines scope for all resource servers
groups	--groups	-G	Groups having access to scope, separated by comma

6.2.1.3.2 Removing Scope

Usage:

```
iasm remove_scope [-N][--name]]
```

Options:

Config Parameter	Option	Short Option	Description
name	--name	-N	Name of scope to be added with ip address of resource server. Format: ip@scope. No ip defines scope for all resource servers.

6.2.1.3.3 Updating Scope Information

Usage:

```
iasm update_scope [-N][--name] [-U][--users] [-G][--groups]
```

Options:

Config Parameter	Option	Short Option	Description
name	--name	-N	Name of scope to be added with ip address of resource server. Format: ip@scope. No ip defines scope for all resource servers.
scopes	-scopes	-S	Scopes to which client will have an access separated by comma. Scope format: ip@scope. No ip defines scope for all resource servers
groups	--groups	-G	Groups having access to scope, separated by comma

6.2.1.4 List Commands

List queried parameters.

Usage:

```
iasm list [-C][--clients] [-S][--scopes] [-U][--users] [-G][--groups]
```

Options:

Config Parameter	Option	Short Option	Description
clients	--clients	-C	List clients
scopes	--scopes	-S	List scopes
users	--users	-U	List users
groups	--groups	-G	List groups

6.3 Configuration File Structure

Intel Accelerated Storage Manager uses iasm.conf file to store and read configuration. This file is placed in /etc/iasm/ directory on Linux.

After each file modification, service restart is required.

Default *iasm.conf* file presented below

```
[config]
host = localhost
port = 80
http_threads = 16
plugins_threads = 8
plugins_timeout = 300
https = false
certificate = non
web_server = false
web_content = non
oa_auth_provider = local
oa_server = false
oa_server_host = localhost
oa_server_port = 80
oa_grants = implicit,code
oa_token_expiration_time = 3600
oa_code_expiration_time = 30
oa_refresh_expiration_time = 7200

[client]
client_id = "Intel Accelerated Storage Manager"
scopes = info,vroc,ssd
grants = implicit,code

[scope]
name = info

[scope]
name = vroc

[scope]
name = ssd
```

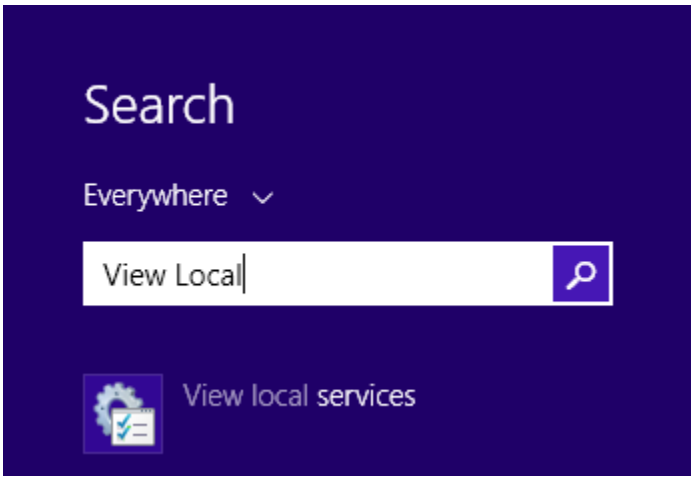
6.4 Managing the Service

After installation, Intel Accelerated Storage manager is up and running with startup type set to 'Automatic'. This means, that service will start along with OS start.

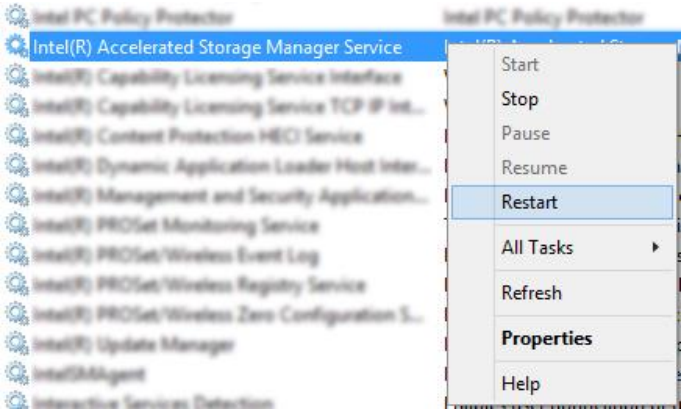
However, after each modification of configuration file, user need to restart the service.

Starting and stopping can be done through Windows* Local Services manager.

Restarting Intel® ASM Service:

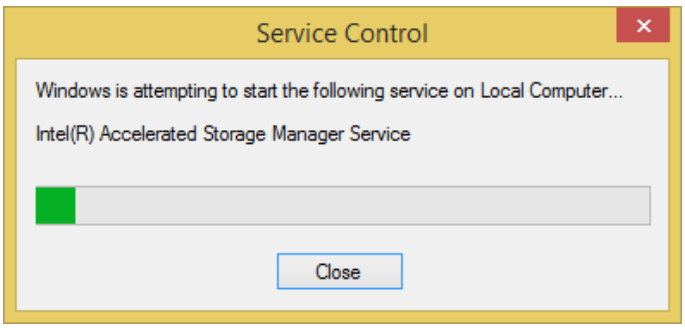


To restart the service, press windows button and start typing "View Local" and click on the "View Local Services" item.



In services window locate and select the "Intel Accelerated Storage Manager Service".

Click on selected item with right mouse button and select "Restart" from context menu.



System will display notification about stopping and starting the service.

6.5 Standalone Configuration Example

This section contains an example standalone configuration of Intel Accelerated Storage Manager. All application components will be installed and configured on one server machine.

Installation of Intel ASM for remote management requires system with configured network interface.

6.5.1 Assumptions

- **All used IP addresses are examples only (except 127.0.0.1).**
- Platform used **must** support VROC 6.0.
- Server machine contains a Windows* operating system already installed.
- Machine IP address is 10.100.100.10 (To configure service locally, on machine without network access, 127.0.0.1 loopback address should be used).
- Intel ASM Server will be configured to use machine IP address and 8080 port.
- User that will perform all configuration steps (admin) has administrator privileges.

6.5.2 Windows* Installer and Configuration

By default in Windows* install all the parameters are set apart from adding the user scope to grant access to "admin" user (In windows the admin user is the one used to log into the system):

```
C:\Program Files\Intel\Intel Accelerated Storage Manager> iasm update_scope -N vroc -U admin
C:\Program Files\Intel\Intel Accelerated Storage Manager> iasm update_scope -N info -U admin
C:\Program Files\Intel\Intel Accelerated Storage Manager> iasm update_scope -N ssd -U admin
```

6.5.3 Silent Installation

Copy the Rapid Storage Technology enterprise installer file (SetupVROC.exe) to the desired directory ("C:\" in this example).

Run the silent installation:

```
C:\>SetupVROC.exe –s –IASM_INSTALL_IN_SILENT –IASM_WEB_SERVER_INSTALL
```

6.5.4 Configuration

Configuring Intel ASM Service

All configuration presented below can be done by manually editing "*C:\Program Files\Intel\Intel Accelerated Storage Manager\iasm.conf*" file. This file contains also commented entries for all available application scopes.

Configure HTTP service to listen on 10.100.100.10 address, under 8080 port, enable WWW server capability and provide valid path to Intel ASM GUI:

```
C:\Program Files\Intel\Intel Accelerated Storage Manager> iasm config -I 10.100.100.10 -P 8080
C:\Program Files\Intel\Intel Accelerated Storage Manager> iasm config -S true -D C:\Program
Files\Intel\Intel Accelerated Storage Manager\www\
```

For the localhost configuration:

```
C:\Program Files\Intel\Intel Accelerated Storage Manager> iasm config -I 127.0.0.1 -P 8080
C:\Program Files\Intel\Intel Accelerated Storage Manager> iasm config -S true -D C:\Program
Files\Intel\Intel Accelerated Storage Manager\www\
```

Update required scopes to grant access to *"admin"* user:

```
C:\Program Files\Intel\Intel Accelerated Storage Manager> iasm update_scope -N vroc -U admin
C:\Program Files\Intel\Intel Accelerated Storage Manager> iasm update_scope -N info -U admin
C:\Program Files\Intel\Intel Accelerated Storage Manager> iasm update_scope -N ssd -U admin
```

Configuring Intel ASM Management Console

Open GUI configuration file (config.json) for editing i.e. using notepad application.

Edit file by adding resource server URI, in this example, for standalone configuration this should point to current server IP and port.

After modifications GUI configuration file should look like this:

```
{
    "AUTHORIZATION_URL": "",
    "RESOURCE_SERVER_ARRAY": ["http://10.100.100.10:8080"],
    "API_VERSION": "v1",
    "PLUGINS_PATH": "source/plugins/",
    "APPLICATION_IDENTIFIER": "Intel Accelerated Storage Manager"
}
```

For the localhost configuration:

```
{
    "AUTHORIZATION_URL": "",
    "RESOURCE_SERVER_ARRAY": ["http://127.0.0.1:8080"],
    "API_VERSION": "v1",
    "PLUGINS_PATH": "source/plugins/",
    "APPLICATION_IDENTIFIER": "Intel Accelerated Storage Manager"
}
```

Starting and Testing Configuration

Restart Intel ASM Service:

```
C:\Program Files\Intel\Intel Accelerated Storage Manager> net stop IntelASMService
C:\Program Files\Intel\Intel Accelerated Storage Manager> net start IntelASMService
```

Test configuration by navigating to "http://10.100.100.10:8080" or "http://127.0.0.1" (in case of localhost configuration) URI in web browser.

As a username and password, use previously configured user with his corresponding system password (admin).

6.6 Distributed Configuration Example

As described in **Error! Reference source not found.** Intel Accelerated Storage manager can be configured to work on multiple servers with one or many authentication end points and one or many application servers.

Installation of Intel ASM for remote management requires system with configured network interface.

6.6.1 Assumptions

Example configuration assumes that (Figure 4):

- **All used IP addresses are examples only (except 127.0.0.1).**
- Network configuration contains at least one domain controller against which all Intel ASM Clients will be authenticated (domain example.com),
- There are two users configured on Domain Controller that will be authorized for Intel ASM services with logins: "*jeff*" and "*esmond*".
- All resource servers will be authenticated against one Intel ASM authentication service – this target machine is joined to domain "*example.com*",
- One Intel ASM service will work in application server mode, where Intel ASM management console will be hosted,
- There are two Intel ASM services working in resource server mode.

Figure 4: Example of Distributed Configuration

6.6.2 Authentication Server Configuration

Installing Components

Copy the Rapid Storage Technology enterprise installer file (SetupVROC.exe) to the desired directory ("C:\" in this example).

Run the silent installation:

```
C:\>SetupVROC.exe –s –IASM_INSTALL_IN_SILENT
```

Configuring Authentication Service

For configuration, use following commands or manually edit "*C:\Program Files\Intel\Intel Accelerated Storage Manager\iasm.conf* " file.

Configure HTTP service to listen on 10.100.199.11 address, under 80 port:

```
C:\Program Files\Intel\Intel Accelerated Storage Manager> iasm config -I 10.100.100.11 -P 80
```

Configure Intel ASM to use domain authentication:

```
C:\Program Files\Intel\Intel Accelerated Storage Manager> iasm config -V domain
```

Update required scopes to grant user access:

```
C:\Program Files\Intel\Intel Accelerated Storage Manager> iasm update_scope -N vroc -U jeff@example.com
C:\Program Files\Intel\Intel Accelerated Storage Manager> iasm update_scope -N vroc -U esmond@example.com
C:\Program Files\Intel\Intel Accelerated Storage Manager> iasm update_scope -N info -U jeff@example.com
C:\Program Files\Intel\Intel Accelerated Storage Manager> iasm update_scope -N info -U esmond@example.com
C:\Program Files\Intel\Intel Accelerated Storage Manager> iasm update_scope -N ssd -U jeff@example.com
C:\Program Files\Intel\Intel Accelerated Storage Manager> iasm update_scope -N ssd -U esmond@example.com
```

Starting Authorization Service

Restart Intel ASM service:

```
C:\Program Files\Intel\Intel Accelerated Storage Manager> net stop IntelASMService
C:\Program Files\Intel\Intel Accelerated Storage Manager> net start IntelASMService
```

6.6.3 Application Server Configuration

Installing Components

Copy the Rapid Storage Technology enterprise installer file (SetupVROC.exe) to the desired directory ("C:\" in this example).

Run the silent installation:

```
C:\>SetupVROC.exe -s -IASM_INSTALL_IN_SILENT -IASM_WEB_SERVER_INSTALL
```

Configuring HTTP Service

For configuration, use following commands or manually edit "*C:\Program Files\Intel\Intel Accelerated Storage Manager\iasm.conf*" file.

Configure HTTP service to listen on 10.100.100.12 address, under 80 port, enable WWW server capability and provide valid path to Intel ASM GUI:

```
C:\Program Files\Intel\Intel Accelerated Storage Manager> iasm config -I 10.100.100.12 -P 80
C:\Program Files\Intel\Intel Accelerated Storage Manager> iasm config -S true -D C:\Program
Files\Intel\Intel Accelerated Storage Manager\www\
```

Configuring Intel ASM Management Console

Open GUI configuration file (config.json) for editing i.e. using notepad application.

Edit file by adding previously configured authorization server URI (10.100.100.11) and by adding resource server URIs, in this example 10.100.100.13 and 10.100.100.14.

After modifications, GUI configuration file should look like this:

```
{
    "AUTHORIZATION_URL": ""http://10.100.100.11:80",
    "RESOURCE_SERVER_ARRAY": ["http://10.100.100.13:80", "http://10.100.100.14:80"],
    "API_VERSION": "v1",
    "PLUGINS_PATH": "source/plugins/",
    "APPLICATION_IDENTIFIER": "Intel Accelerated Storage Manager"
}
```

Starting Application Service

Restart Intel ASM service:

```
C:\Program Files\Intel\Intel Accelerated Storage Manager> net stop IntelASMService
C:\Program Files\Intel\Intel Accelerated Storage Manager> net start IntelASMService
```

6.6.4 Resource Servers Configuration

Perform those steps for each resource server machine.

Installing Components

Copy the Rapid Storage Technology enterprise installer file (SetupVROC.exe) to the desired directory ("C:\" in this example).

Run the silent installation:

```
C:\>SetupVROC.exe –s –IASM_INSTALL_IN_SILENT
```

Configuring HTTP Service

For configuration, use following commands or manually edit "*C:\Program Files\Intel\Intel Accelerated Storage Manager\iasm.conf* " file.

Configure HTTP service to listen on 10.100.100.13 address, under 80 port:

```
C:\Program Files\Intel\Intel Accelerated Storage Manager> iasm config -I 10.100.100.13 -P 80
```

Configure Intel ASM to use previously configured authentication server (10.100.100.11:80):

```
C:\Program Files\Intel\Intel Accelerated Storage Manager> iasm config -A true -O 10.100.100.11 -T 80
```

Starting Resource Service

Restart Intel ASM service:

```
C:\Program Files\Intel\Intel Accelerated Storage Manager> net stop IntelASMService
C:\Program Files\Intel\Intel Accelerated Storage Manager> net start IntelASMService
```

Repeat these steps for 10.100.100.14 machine.

6.6.5 Testing Configuration

To test configuration, navigate in your web browser to application server (http://10.102.108.12), select one resource servers from the drop down list and click "Sign In" button.

Browser should navigate you to login page located on 10.100.100.11 machine.

Enter user credentials with domain name i.e.

- Username: jeff,
- Password: [jeff's password],
- Domain: example.lab,

Then click "Sign In".

After successfully logging in, browser should redirect user back to 10.100.100.12 displaying Intel ASM Management Consoles Dashboard for selected resource server.

§

7 REST API

Intel Accelerated Storage Manager released with VROC 6.0 provides REST API for four different scopes:

- Security requests – set of functions providing OAuth 2.0 authentication capability.
- System Information – general set of information about platform where service is installed.
- SSD API – set of information about connected and supported storage devices.
- VROC API – set of management and informational functions for VROC 6.0 product.

Detailed information about requests and responses format are available in referenced documents:

- Intel ASM Security REST API.pdf
- Intel ASM System Plugin REST API.pdf
- Intel ASM SSD Plugin REST API.pdf
- Intel ASM VROC Plugin REST API.pdf

§

8 Intel VROC 6.0 Wed GUI

8.1 Getting Started

8.1.1 Configuration

Web GUI settings are configured in config.json file. The file is located in the www directory.

After file modification service restart is required.

Web GUI configurables:

- Authorization URL – address of Oauth2.0 authorization server used by GUI to authenticate a user.
- API version – REST API version
- Application identifier – GUI ID used for application identification to authorization server ("client_id" from the iasm.conf file)
- Resource servers array – List of resource servers (servers' URLs with RESTful Service)
  Resource server is an operating ASM service that exposes REST API through HTTP or HTTPS that allows Web GUI to fetch necessary data.
  Multiple Resource server URLs may be defined allowing user to quickly navigate through and manage different machines.

Example of *config.json* file presented below.

```
{
  "AUTHORIZATION_URL": "http://10.100.100.100:8080",
  "API_VERSION": "v1",
  "APPLICATION_IDENTIFIER": "Intel Accelerated Storage Manager",
  "PLUGINS_PATH": "source/plugins/",
  "RESOURCE_SERVER_ARRAY": [
    "http://10.100.100.100:8080",
    "http://10.100.100.101:8080"
  ]
}
```

8.1.2 Supported Browsers

- Google Chrome (version 50.0.2661+)
- Mozilla Firefox (version 42.0+)
- Internet Explorer 11+

8.1.3 Web Page Responsiveness

Web page is responsive, therefore it can be accessed by all devices of all sizes from mobile phones through large monitors with comparable level of user experience.

Due to performance considerations, some functionalities are unavailable on mobile devices.

There include dashboard edition. Memory, and CPU performance monitoring.

8.1.4 Cookies

Application's session data is stored in cookies.

Browser's cookies are requires for web page to work.

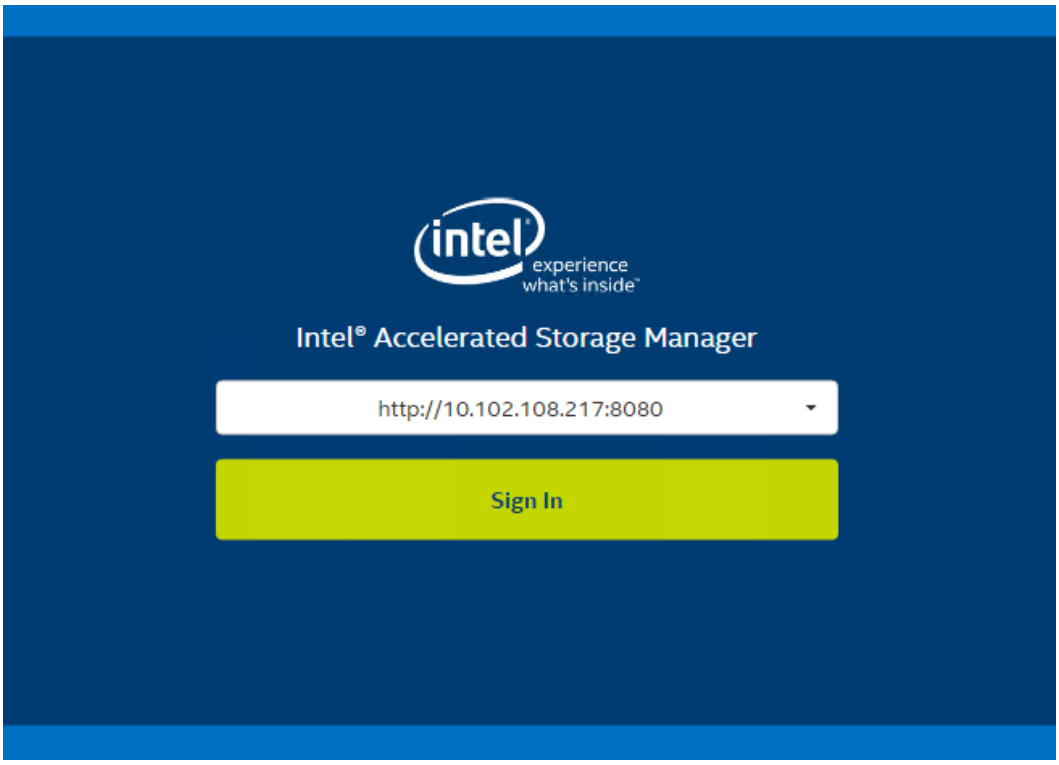
Disallowing cookies or removing them manually will log off a user.

8.2 Login Page

User requests access to the resource server by selecting it from dropdown menu.

List of available resource servers is configured in config.json file.

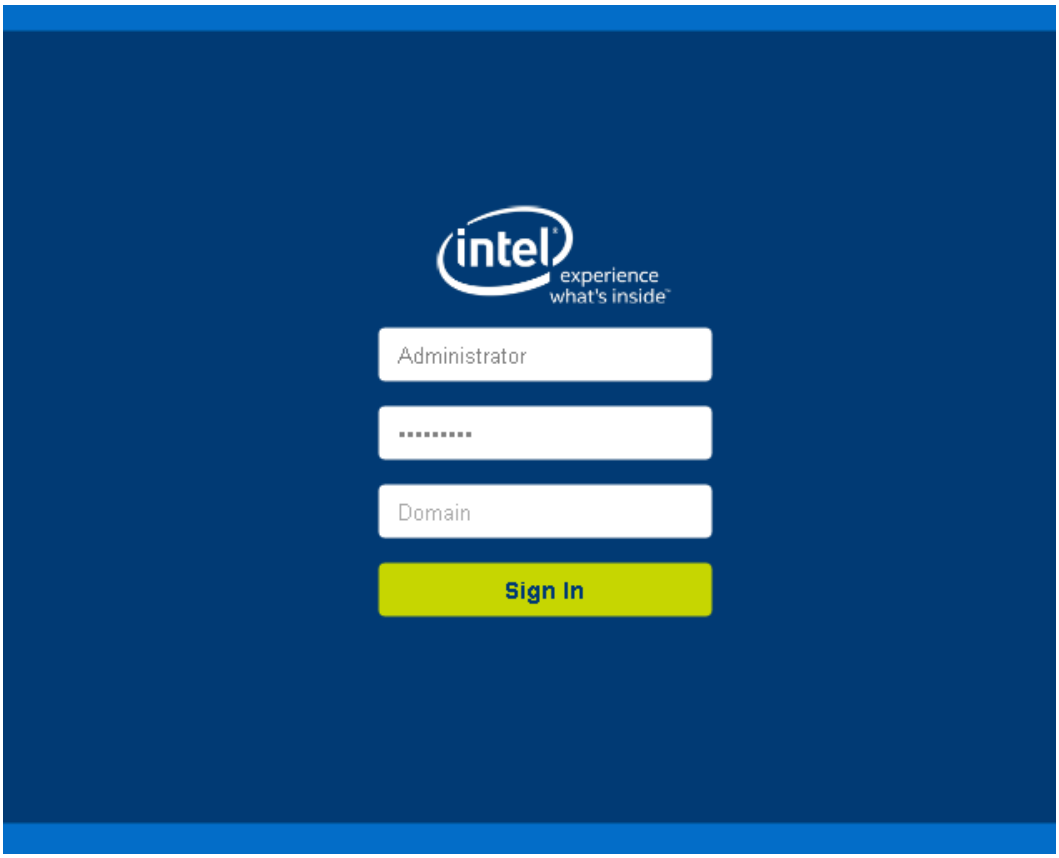
There has to be at least one resource server defined to gain access to the application.
Authorization server cannot be selected from login page. It has to be configured in config.json file. If "AUTHORIZATION_URL" configurable is left blank, resource server is assumed to act as authorization server as well.



"Sign In" button redirects user to the login form served by the authentication server.

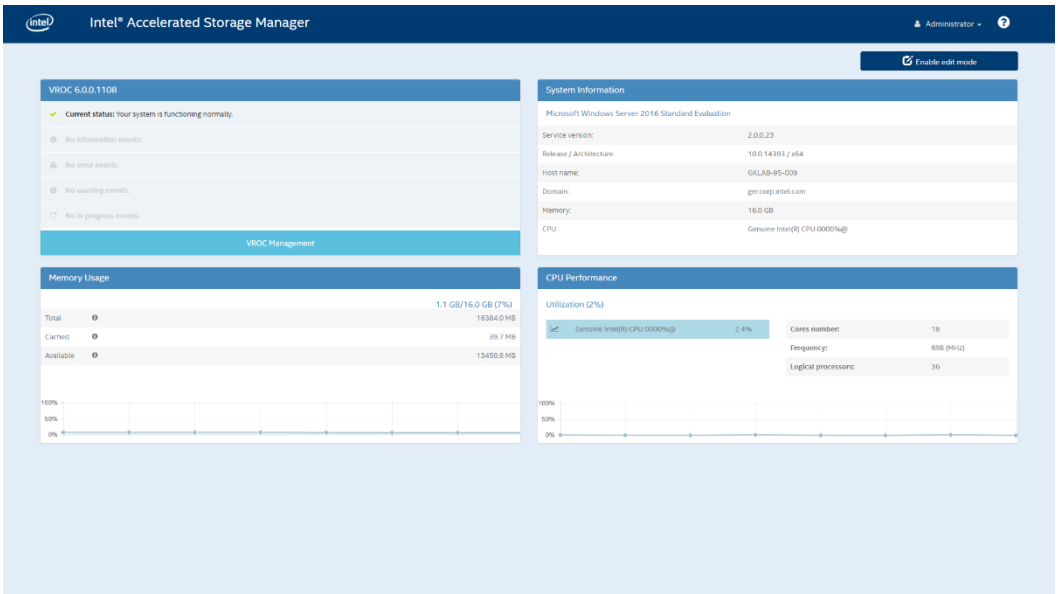
User shall authenticate himself with system or domain credentials depending on Intel ASM configuration.

"Domain" field is mandatory when user authenticates against Active Directory Domain Services, otherwise field should remain empty.



Once the submitted credentials are confirmed, the user is redirected back to the application, where application dashboard is displayed.

8.3 Dashboard



This is the main page of the web application. Users always have the option to navigate back to the dashboard by clicking on the INTEL logo in the upper left corner, or by selecting the “Home” option in the dropdown menu in the upper right corner.

Dashboard is editable; therefore, user may configure widgets’ order and composition on the screen. To edit dashboard click “Enable edit mode” button and confirm changes once done.

Dashboard settings are stored in browser’s Local Storage; hence, are not lost upon browser closure.

8.3.1 System Widget

System Widget presents basic information about the system, on which the resource server is located.

8.3.2 Memory Widget

Memory Widget presents memory data such as total, cached, and available memory. Real-time memory usage is presented on the graph.

8.3.3 CPU Performance Widget

CPU Performance Widget presents basic processor information.

Real-time CPU usage is presented on the graph. Each processor usage is shown as a separate plot.

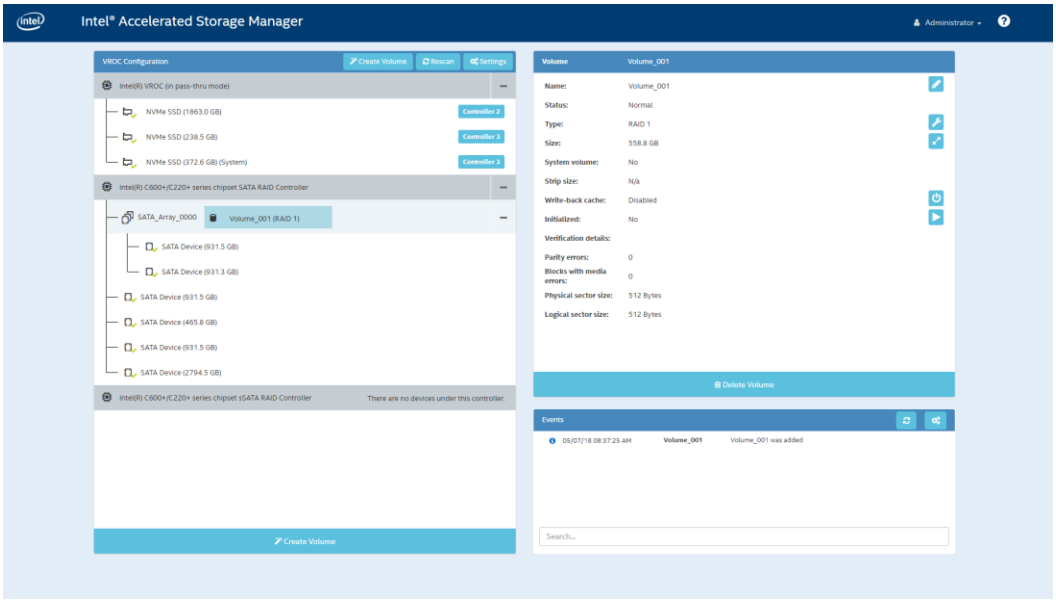
8.3.4 VROC Management Widget

VROC Management Widget indicates whether VROC is functioning normally.

8.4 VROC Management

VROC Management is divided into three sections:

- Tree View
- Element Details View
- Events Log



8.4.1 Tree View

Tree View presents Controllers, Arrays, Volumes, and EndDevices. This guide will refer to them as components. Controllers and Arrays can be collapsed to simplify the view if needed.

Aforementioned components are selectable. Selecting a component displays its details on the right side of the page in Details View.

8.4.2 Details View

This view contains detailed component information along with action buttons associated with them.

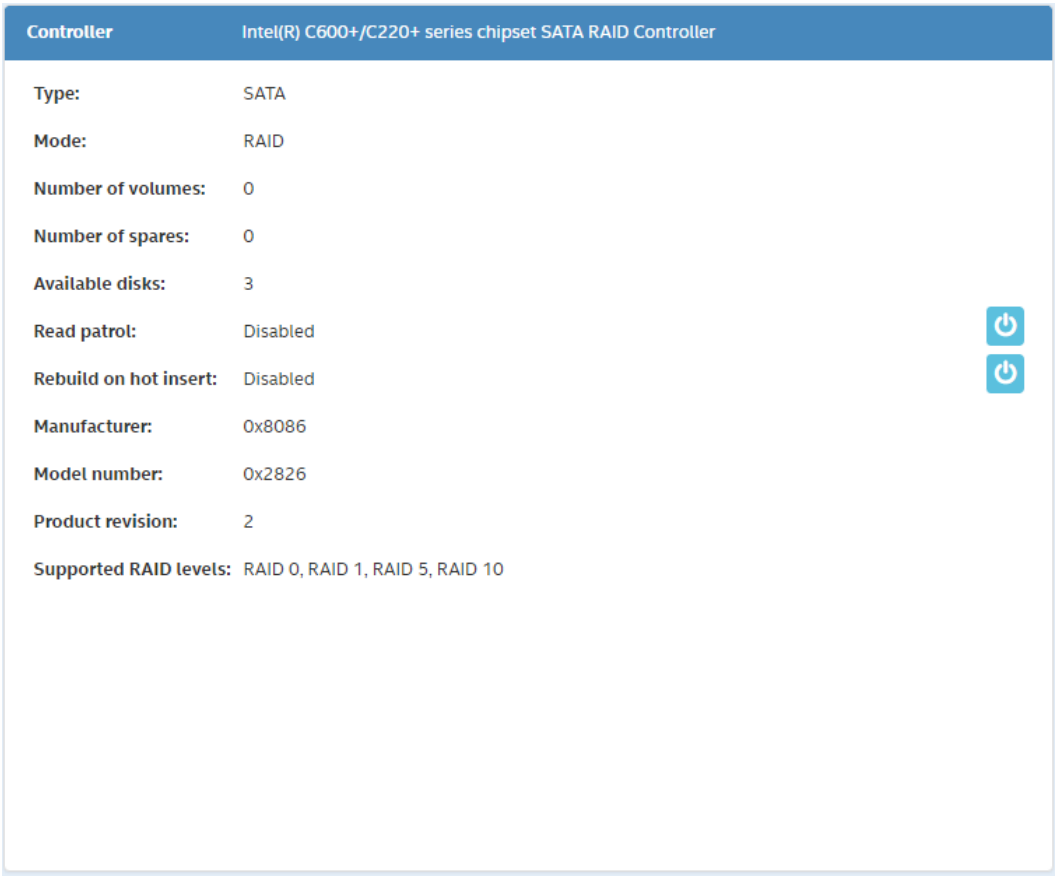
Displayed data and action buttons vary with every component.

Action buttons are displayed only when given action may be performed. Buttons are located next to the field they have impact on. Example: “Rename” button stands next to “Volume Name” field.

Complete list of action can be found below.

Help module describes these actions in more details.

8.4.2.1 Controller Details



Controller actions:

- Toggle Read Patrol
- Rebuild on Hot Insert on/off

8.4.2.2 Array Details

Array actions:

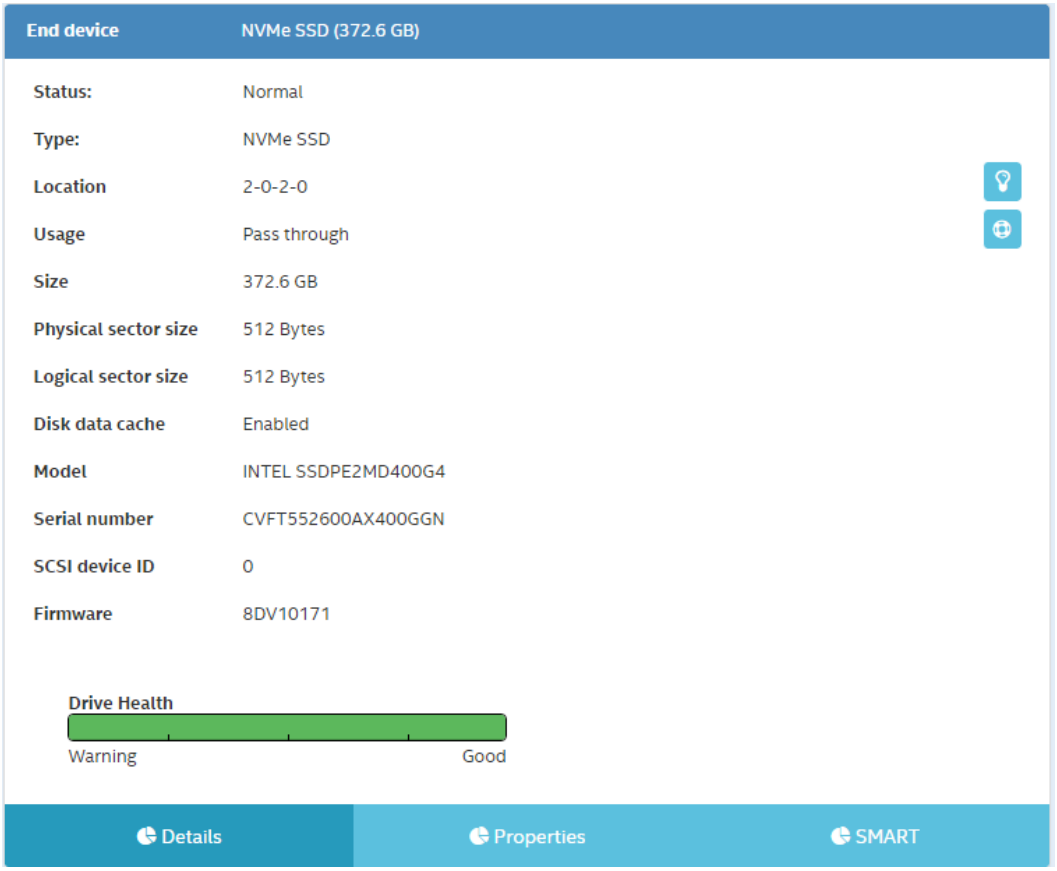
- Add disk to Array
- Enable/Disable Array Cache Policy

8.4.2.3 Volume Details

Volume actions:

- Rename Volume
- Rebuild Volume
- Mark Volume as Normal (Clear Volume Metadata)
- Change Volume Type (Raid Level migration)
- Change Volume Size
- Enable/Disable Write-back Cache Policy
- Change Close RAID Write Hole (RWH) policy
- Initialize Volume
- Verify/Verify and Fix
- Delete Volume

8.4.2.4 EndDevice Details



EndDevice actions:

- Mark disk as Normal
- Clear Metadata
- Activate LED/toggle LED
- Mark as Spare

There are two more tabs that are enabled only if SSD Plugin is installed.

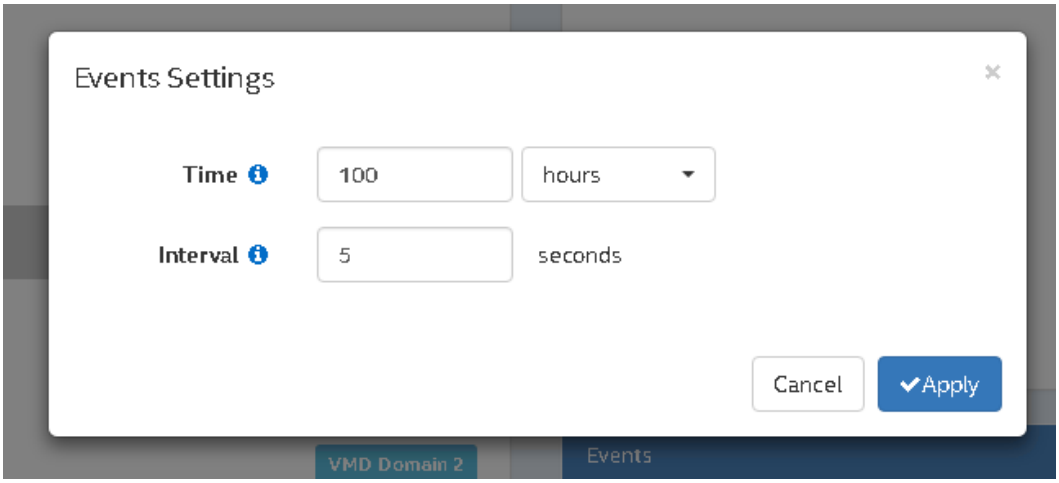
- Properties – collection of drive properties and health data.
- S.M.A.R.T. – collection of S.M.A.R.T. data

8.4.3 Events Log

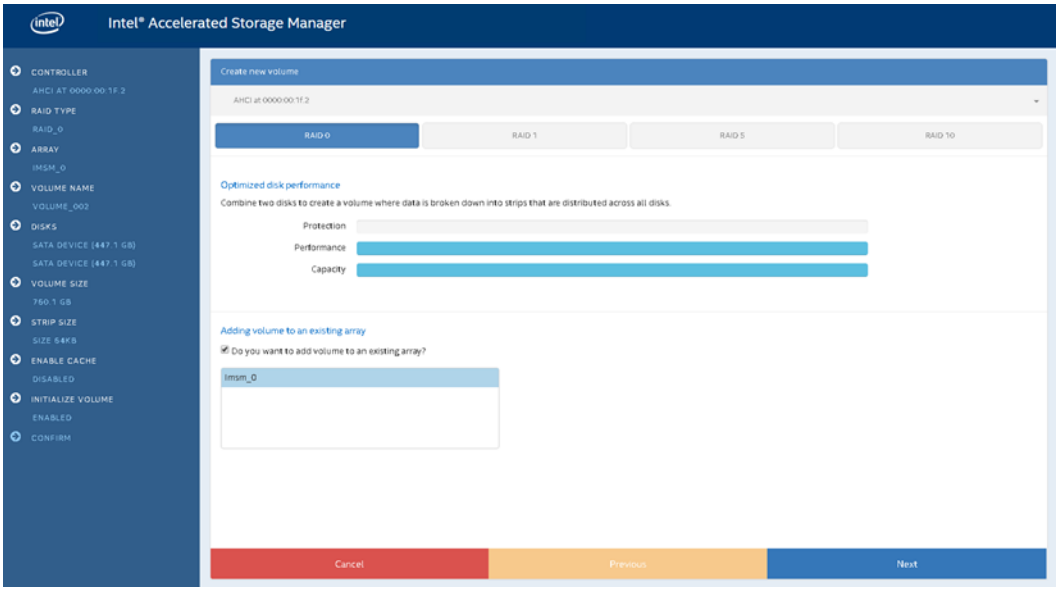
Events log is a list of predefined events that ASM Service has reported.

Events log displays all events including those not triggered by the webpage user.

User may configure how frequently wants to update events log and what time depth should be.



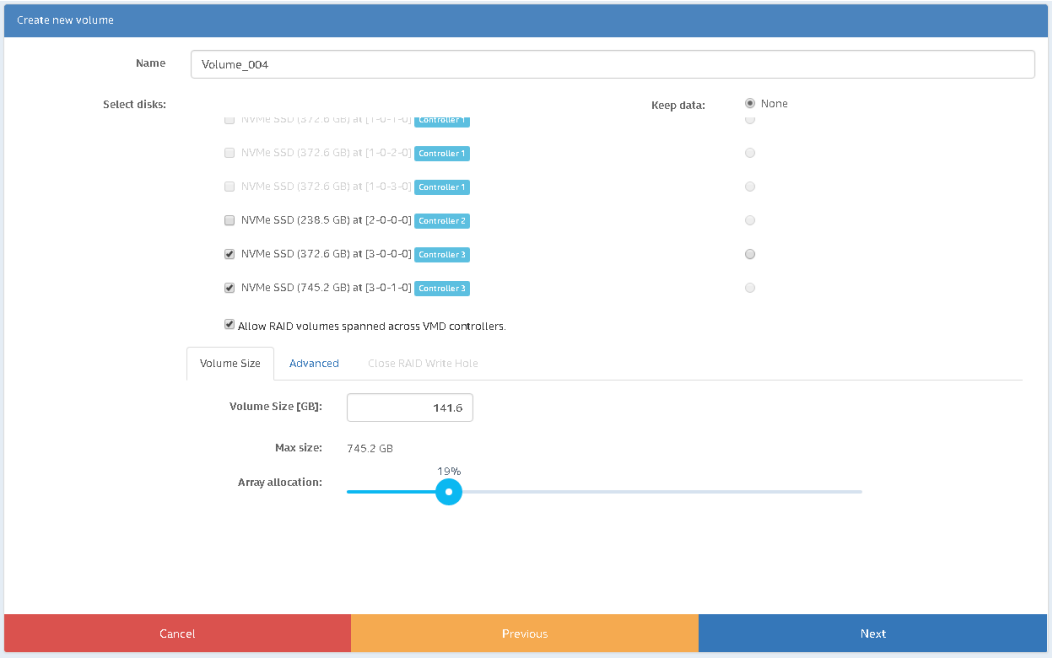
8.4.4 Create New Volume Wizard



The process of creating new volume consists of several steps.
Each step's possible selection may be dependent on the selections made in previous steps; therefore, it is highly recommended to work the process page by page, from top to bottom.

Steps:

- Select Controller:
  - Select controller, on which new Volume shall be created. Controller has to be in RAID mode.
- Select RAID Level:
  - Select RAID Level for new volume. There are four RAID levels available: RAID0, RAID1, RAID5, and RAID10. RAID description can be found below RAID selection.
    Note: Key version determines which RAID levels can be created on a platform. These are as follows:
    - VROC (in pass-thru mode): RAID0
    - VROC STANDARD: RAID0, RAID1, RAID10
    - VROC PREMIUM: RAID0, RAID1, RAID5, RAID10
- Add volume to already existing array or create volume in a new array:
  - Volume is created in a container called array. There is a possibility of creating up to two volumes in single array (Matrix RAID configuration). User may choose to create a volume in a new array or to add it to an already existing array. If user choose to add a new volume to an already existing array, most following options are blocked and cannot be altered.



- Name new Volume
  - User may choose a name for the volume. Default name will be given, if user chooses not to do so.
- Select Disks to be included in a new volume
  - RAID0 – select at least two disks
  - RAID1 – select exactly two disks
  - RAID5 – select at least three disks
  - RAID10 – select exactly four disks

Note: While creating volume on VMD Controller, it is possible to create volume from disks located in different VMD Domains. User has to explicitly confirm that he wants to create such volume by checking “Allow VMD Spanning” checkbox.
Wizard blocks user from proceeding until disks are selected.

- Choose to Keep Data from Disk (supported on Windows only)
  - User may choose to save data from one of selected disks.
  - Data from system drive is always selected.
  - If Keep Data option is selected, Volume Size is always set to 100%
- Set Volume Size
  - User may set volume’s size. This can be done either by slider or by manual input.
- Select Strip Size
  - Select volume Strip Size. Recommended Strip Size is set by default.
- Enable Volume Write-back Cache
  - This action can be done once volume is created
- Initialize Volume
  - This action can be done once volume is created
- Select Close RAID Write Hole policy
  - Available RAID Write Hole policies are OFF, DISTRIBUTED, JOURNALING DRIVE (supported on Windows only)

§