

INTEL-SA-00075 Detection and Mitigation Tool Guide

Intel® Active Management Technology (Intel® AMT), Intel® Standard Manageability (ISM), and Intel® Small Business Technology (SBT)

Instructions for detecting and mitigating INTEL-SA-00075

Revision 1.0 – June 6, 2017

Introduction

This document will step you through multiple processes to detect and mitigate the security vulnerability described in INTEL-SA-00075. Read the Public Security Advisory at <https://security-center.intel.com/advisory.aspx?intelid=INTEL-SA-00075&languageid=en-fr> for more information.

If you are a user of a single PC and you wish to determine its status: We provide the INTEL-SA-00075 Detection GUI application (Intel-SA-00075-gui.exe) for local analysis of a single or standalone system.

If you want to determine the status and/or apply mitigations for multiple machines: We have provided the INTEL-SA-00075 Detection and Mitigation Tool console (Intel-SA-00075-console.exe) application. This tool can perform discovery and write its findings to the local Windows Registry, and (optionally) to an XML file, for subsequent collection and analysis. The console application can also assist in implementing mitigations. See *Using the INTEL-SA-00075 Detection and Mitigation Tool* on page 2 for more information.

If you are a network administrator who is already using the Intel® Setup and Configuration Software (Intel® SCS): The Intel® SCS suite contains an alternative, console tool, the Intel® SCS System Discovery utility. We suggest use of this tool if you are already familiar with Intel® SCS tools or would like to get detailed data about Intel® AMT. See *Using the Intel® SCS System Discovery Utility* on page 10.

Mitigation

The mitigation steps described in this document are intended to prevent unauthorized activation and use of Intel manageability SKUs, Intel® Active Management Technology (Intel® AMT), Intel® Standard Manageability (ISM), and Intel® Small Business Technology (SBT), that have not applied the firmware update addressing the vulnerability.

IT practitioners can use these instructions as basis for scripts or tasks within management consoles for scale deployments of the mitigation steps. The procedural steps for implementing the mitigation are as follows:

1. Unprovisioning Intel manageability SKU clients to mitigate unprivileged network attacker from gaining system privileges
2. Disabling or removing the Local Manageability Service (LMS) to mitigate unprivileged local attacker from gaining system privileges
3. Optionally configuring local manageability configuration restrictions

Intel highly recommends that the first step in all mitigation paths is to unprovision the Intel manageability SKU to address the network privilege escalation vulnerability. For provisioned systems, unprovisioning must be performed prior to disabling or removing the LMS. Pending availability of the updated Intel manageability SKU firmware, Intel highly recommends mitigation of the local privilege escalation by removing or disabling the LMS. Optionally, as a second layer of defense against inadvertent reinstall or re-enabling of the LMS, some of the manageability configuration options performed through the OS can additionally be disabled through the operating system (OS); however, these additional local manageability configuration restrictions have constraints on how they are allowed to be reversed.

For assistance in implementing the mitigation steps provided in this document, please contact [Intel Customer Support](#); from the Technologies section, select Intel® Active Management Technology (Intel® AMT).

Using the INTEL-SA-00075 Detection and Mitigation Tool

What is the INTEL-SA-00075 Detection and Mitigation Tool?

The INTEL-SA-00075 Detection and Mitigation Tool can be used by local users or an IT administrator to determine whether a system is vulnerable to the exploit documented in Intel Security Advisory INTEL-SA-00075. The console version of the tool can be used to perform mitigation steps.

The Detection and Mitigation Tool is offered in two versions.

- The first is an interactive GUI tool that, when run, discovers the hardware and software details of the device and provides indication of risk assessment. This version is recommended when local evaluation of the system is desired.
- The second version is a console executable that can perform the risk assessment and perform recommended mitigation steps. It can optionally save the discovery information to the Windows* registry and/or to an XML file. This version is more convenient for IT administrators wishing to perform bulk discovery and mitigation operations across multiple machines.

Obtaining the INTEL-SA-00075 Detection and Mitigation Tool

The INTEL-SA-00075 Detection and Mitigation Tool download package is available at:
<https://www.intel.com/content/www/us/en/support/technologies/000024133.html>.

System requirements

- Microsoft Windows* 7, 8, 8.1, or 10
- Local operating system administrative access

Installing the tool

Interactive installation

Run INTEL-SA-00075 Detection and Mitigation Tool.msi and follow the prompts on the screen.

Silent installation

```
msiexec.exe /i INTEL-SA-00075 Detection and Mitigation Tool.msi /qn
```

This will install the INTEL-SA-00075 Detection and Mitigation Tool in the default directory, C:\Program Files (x86)\Intel\Intel-SA-00075 Detection and Mitigation Tool\

Uninstalling the tool

Interactive uninstallation

Run INTEL-SA-00075 Detection and Mitigation Tool.msi and follow the prompts on the screen.

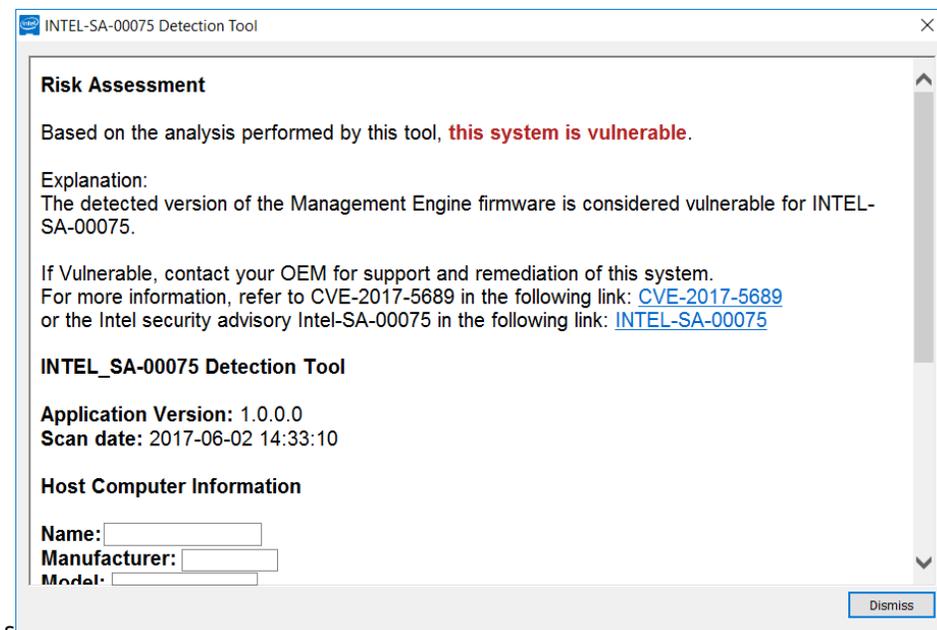
Silent uninstallation

```
msiexec.exe /x INTEL-SA-00075 Detection and Mitigation Tool.msi /qn
```

Running the GUI tool

INTEL-SA-00075-GUI.exe is designed to run on a single system. When run, the tool outputs the discovery information to the screen.

Figure 1. Example of INTEL-SA-00075-GUI output to screen



Running the console tool

Execute `INTEL-SA-00075-console.exe` from a command prompt with administrative rights.

Usage:

```
Intel-SA-00075-console.exe [[command] | [option...]]
```

Only one command may be run at once. If no command is given, the discover command is run.

Table 1. INTEL-SA-00075 console command line switches

Command Line Command	Functionality
-Discover	Output results to the console and write data to the registry.
-Unprovision [password], -u [password]	Remove all Intel AMT settings and disable Intel AMT features, an optional admin user password for the Intel AMT device may be used.
-DisableClientControlMode, -DisableCCM	Permanently disables the Client Control mode option in the Intel AMT device. After running this command, the device cannot be put in Client Control mode. NOTE: There is no CLI command to reverse this action. WARNING: Not all platforms can re-enable CCM once disabled.
-DisableLMS	Disables the LMS service.

Command Line Option	Functionality
-n, -noregistry	Prevents writing results to the registry
-c, -noconsole	Prevents results from being displayed on the console
-d, -delay <seconds>	Delay in seconds before execution starts. If no value is specified, the tool will have no delay.
-f, -writefile	Specifies writing results to a file. The filename uses the following format: <computername>.xml
-p <filepath>, -filepath ,<filepath>	The path to store the output file. If no path is specified, the file will be written to the directory that the tool is running from.
-h, -help, -?	Displays these command line switches and their functions

-Discover

The discover command displays outputs the discovery information to the console. By default it also writes discovery data to the registry. If no command is given to the console tool, discover is the run.

-Unprovision

Remove all Intel AMT settings and disable Intel AMT features, an optional admin user password for the Intel AMT device may be used.

When configured, Intel® AMT and ISM automatically listen for management traffic over your computer network. Systems that are vulnerable to the known privilege escalation issue should be unprovisioned using the unprovision command to prevent unauthorized access to manageability features. The admin password is optional.

-DisableClientControlMode

The `-DisableClientControlMode` configuration restriction is an optional step for customers that require a secondary layer to protect against mitigation reversal by an unprivileged attacker who gains OS admin privileges. Reversal of these options are difficult, may not be supported by the computer's manufacturer, and may require physical access to the system. If you choose to perform this additional configuration restriction, it must be performed prior to disabling the LMS service

Steps to re-enable CCM

If supported by your manufacturer, you may be able to reset Intel manageability SKUs from BIOS, which would re-enable CCM. Consult your manufacturer to see if this capability is supported and for the steps to follow.

Note: Your manufacturer may provide tools that allow you to configure BIOS settings through the OS. These tools, if available, may allow you to reset Intel manageability SKUs in BIOS without having to physically touch the computer. Check with your manufacturer to see if they provide a tool with this functionality.

-DisableLMS

The DisableLMS command disables the LMS service as a mitigation step.

What is LMS?

Intel® Management and Security Application Local Management Service (LMS) is a service that enables local applications running on Intel® AMT, Intel® SBA or Intel® Standard Manageability supported devices to use common SOAP and WS-Management functionality. It listens to the Intel® Manageability Engine (ME) ports (16992, 16993, 16994, 16995, 623, and 664) and routes the traffic to the firmware through the Intel® MEI driver.

Additional considerations

Anyone with OS administrative privileges will be able to reinstall the LMS if it is removed, or re-enable the service if it is disabled. Therefore, it is important to be cautious to avoid an inadvertent re-install or re-enable of the LMS while the vulnerability exists on the system. For example, the LMS could be reinstalled if you ran the Intel manageability software installer sometime in the future.

Figure 2. Example of INTEL-SA-00075-Console output

```
INTEL-SA-00075 Discovery Tool
Application Version: <app version>
Scan date: <date and time>

*** Host Computer Information ***
Computer Name: <computer name>
Manufacturer: <computer manufacturer>
Model: <computer model>
Processor: <processor model>
Windows Version: <Windows* version>

*** ME Information ***
Version: <Intel ME firmware version>
SKU: <Manageability feature, if any present>
State: <ME provisioning state>
Driver installed: <True/False>
Control Mode: <None/ACM/CCM>
Is CCM Disabled: <True/False/Unknown>
EHBC Enabled <True/False>
LMS state: <Running/Stopped/NotPresent>
MicroLMS state: <Running/Stopped/NotPresent>

*** Risk Assessment ***
Based on the analysis performed by this tool, < this system is vulnerable / this
system is not vulnerable / This system's Firmware has been updated and system is in
unprovisioned state / This system's Firmware has been updated, and system is in
provisioned state / Check with OEM / this system's risk is unknown>

If Vulnerable, contact your OEM for support and remediation of this system.
```

*** For more information ***
 Refer to CVE-2017-5689 at:
<https://nvd.nist.gov/vuln/detail/CVE-2017-5689>
 or the Intel security advisory Intel-SA-00075 at:
<https://security-center.intel.com/advisory.aspx?intelid=INTEL-SA-00075&languageid=en-fr>

The logic used to determine a risk assessment is described in Table 2.

Table 2. Meaning of the Risk Assessment in the output

Message	Meaning
Vulnerable	The detected version of the Management Engine firmware is considered vulnerable for INTEL-SA-00075.
Not Vulnerable	The system meets the "Not Vulnerable" criteria described in <i>Identifying impacted systems using the INTEL-SA-00075 Discovery Tool</i> on page 8.
This system's Firmware has been updated and system is in unprovisioned state	The detected firmware on this system has the fix for INTEL-SA-00075. Ensure that the INTEL-SA-00075 tools were used to perform a full unprovisioning of the system prior to reprovisioning. This will remove any unauthorized configuration settings.
This system's Firmware has been updated, and system is in provisioned state	The detected firmware on this system has the fix for INTEL-SA-00075. If the system was provisioned prior to the firmware update, a full unprovision and reprovision of the system will remove any unauthorized configuration settings.
Check With OEM	The detected information in the SMBIOS from the OEM shows a manageability SKU, but the tool did not receive a response when requesting detailed data from your computer. This may be caused by a missing Management Engine interface driver. Consult your OEM to find out if your computer model is affected.
Unknown	The tool did not receive a valid response when requesting hardware inventory data from your computer. Please contact your system manufacturer for assistance in determining the vulnerability of this system.

Results

Note: The amount of data returned by the INTEL-SA-00075 Discover command will depend on if the Intel manageability driver stack is loaded on to the system. If the Intel® Management Engine Interface (MEI) driver and Intel® Management and Security Application Local Management Service (LMS) are present, there will be a more verbose set of data available. Some of the fields may not be supported by the manufacturer.

Registry Location

The values from the results table can be found in the following registry key:

- 32-bit operating systems: HKLM\SOFTWARE\
Intel\Setup and Configuration Software\INTEL-SA-00075 Discovery Tool
- 64-bit operating systems: HKLM\SOFTWARE\WOW6432Node\
Intel\Setup and Configuration Software\INTEL-SA-00075 Discovery Tool

XML

If you choose to write results to a XML file, that file will be stored in the directory that INTEL-SA-00075-console.exe is executed from or the path specified in the command line options.

Console return codes

Table 3. INTEL-SA-00075 console return codes

Number	Meaning
0	NOTVULNERABLE (If Discover command was run) STATUS_OK
2	MACHINE_STATE_UNCONFIGURED
30	CLIENT_CONFIG_NOT_SUPPORTED
39	DISABLE_CCM_IN_ADMIN_MODE
83	HECI_NOT_INSTALLED
111	HECI_ERROR
500	DISCOVERY__VULNERABLE
501	DISCOVERY_POTENTIALLYVULNERABLE_PROVISIONED
502	DISCOVERY_POTENTIALLYVULNERABLE_UNPROVISIONED
503	DISCOVERY_CHECKWITHOEM
504	DISCOVERY_UNKNOWN_RISK
505	DISCOVERY_UNKNOWN
506	DISCOVERY_UNKNOWN_CPU

Table 4. INTEL-SA-00075 console output values

Value	Location	Description
Application Version		The version of the scanning tool used
Scan Date		The date time the scan took place
Computer Name		The name of the computer scanned
Computer Manufacturer	Hardware Inventory	The computer's manufacturer
Computer Model		The computer's model
Processor		The computer's processor model
ME Version	ME Firmware Information	A string value with the full ME firmware version number in the following format: Major.Minor.Hotfix.Build
ME SKU		If present, the manageability feature on the system
ME Provisioning State		The ME configuration state None Detected Not Provisioned Provisioning in Process Provisioned
ME Driver Installed		True/False value if the MEI driver is present on the computer
EHBC Enabled		True/False value if system is capable of Embedded Host Based Configuration provisioning method
LMS State		Information if the LMS Service is running, not running or not present
MicroLMS State		Information if the Micro LMS Service is running, not running or not present
Control Mode		The ME configuration mode None, ACM, or CCM
Is CCM Disabled		True/False/Unknown status for Client Control Mode being disabled
*** Risk Assessment ***	Risk Assessment	See

Identifying impacted systems using the INTEL-SA-00075 Discovery Tool

Impacted systems are defined as having an affected Intel® Management Engine (ME) firmware version and containing one of three manageability feature sets as defined in Table 5.

Table 5. Criteria to determine if a system is vulnerable to INTEL-SA-00075 using the INTEL-SA-00075 Discovery Tool

Value Name	Vulnerable	Not Vulnerable
ME SKU	Intel® Full AMT Manageability Intel® Standard Manageability Intel® Small Business Advantage(SBA)	ME SKU values not present in the vulnerable list to the left -or- ME SKU values to the left with a firmware version that is not vulnerable
ME Version	ME Versions 6.x.x.x – 11.7.x.x with a build value less than 3000 Example: 9.5.22. 1760	ME Versions: <ul style="list-style-type: none"> • 6.x.x.x – 11.7.x.x with a build value greater or equal to 3000 <ul style="list-style-type: none"> ○ Example: 11.6.27.3264 • 2.x.x.x. – 5.x.x.x • 11.7.x.x or greater

Note: Intel® Small Business Technology (SBT) is the manageability SKU for Intel® Small Business Advantage (SBA).

Extending Microsoft* SCCM Hardware Inventory to include the INTEL-SA-00075 console tool results

If you choose to store the results from the Intel-SA-00075 console tool in the Windows Registry, you can leverage the Microsoft* SCCM hardware inventory extensibility to import the results. This will allow you to build up collections in SCCM to target computers for remediation or firmware updates. To do this, you will need to do the following:

1. Add hardware inventory classes to the SCCM configuration.mof file.
2. Enable these new hardware inventory classes in your client configuration.
3. Create a software package to deploy and run the INTEL-SA-00075 Console Tool (`Intel-SA-00075-console.exe`).
4. Create a task sequence to run the software package.

MOF file modification

Note: If you have a central server in your environment, make the MOF file change on it. Otherwise, make these changes on every one of your primary servers.

1. Locate your configuration.mof file. It is typically found in `\Program Files\Microsoft Configuration Manager\inbox\clifiles.src\hin\`
2. Make a backup copy.
3. Edit the configuration.mof file, scrolling down to the end of the file place the cursor above this line:

```
//=====
// Added extensions end
//=====
```

4. Paste the contents of the MOF file changes from page 13 in this document above the line from step three.

5. Save and close the file.
6. Launch a command prompt running as administrator in the directory with configuration.mof.
7. Run mofcomp without switches targeting the modified configuration.mof file.

Hardware inventory changes

Note: Once made, these changes will need time to propagate to your clients before these new items will appear in the hardware inventory. The amount of time this takes will vary depending on how your environment is configured.

1. Launch the Configuration Manager Console.
2. Administration > Client Settings > Default Client Settings.
3. Right-click Default Client Settings > Properties.
4. Select Hardware Inventory > Set Classes.
5. Click Add.
6. Click Connect.
7. Supply credentials if needed and click Connect.
8. Search for Intel_SA.
9. Check the 3 check boxes and click OK.
10. OK > OK.
11. SCCM records the changes to the Hardware Inventory in the dataldr.log.

Create SCCM package

1. Create the batch file from page 15 and place it in a folder with the INTEL-SA-00075 console tool file.
2. Launch the Configuration Manager Console.
3. Software Library > Packages.
4. Right-click Packages > Create Package.
5. Name: Intel-SA-00075.
6. Check This package contains source files.
7. Browse to package folder from step one.
8. Next.
9. Select Do not create a program.
10. Next > Next > Close.
11. Distribute package to appropriate Distribution Points.

Create SCCM task sequence

1. Launch the Configuration Manager Console.
2. Software Library > Operating Systems.
3. Right-click Task Sequences > Create Task Sequence.
4. Select Create a new custom task sequence.

5. Next.
6. Enter a name of Intel-SA-00075.
7. Next > Next > Close.
8. Right-Click the Intel-SA-00075 task sequence and click Edit.
9. Add > General > Run Command Line.
10. Enter Intel-SA-00075.bat in the Command Line field.
11. Check the Package box and select Browse.
12. Select the previously created Intel-SA-00075 package > OK.
13. Click OK.

Using the Intel® SCS System Discovery Utility

What is the Intel® SCS System Discovery Utility?

The Intel® SCS System Discovery Utility is a component of the Intel® Setup and Configuration Software (Intel® SCS) suite that will provide you with specific details of the hardware and software on a system that support Intel® Active Management Technology (Intel® AMT), Intel® Standard Manageability (ISM), or Intel® Small Business Technology (Intel® SBT). When run, it can save the results to the Microsoft Windows registry and/or an XML file. This information can be used to find systems to target for firmware updates or to implement mitigations.

Obtaining the Intel® SCS System Discovery Utility

The Intel® SCS System Discovery Utility download package is available at <https://downloadcenter.intel.com/download/26691/Intel-SCS-System-Discovery-Utility>.

Determining the manageability firmware version using the Intel® SCS System Discovery Utility

The output of the Intel® SCS System Discovery Utility can be used to determine a system's firmware version and if the system is a manageability SKU. This information is provided in the `ManageabilityInfo` section of the output. For instructions on executing the tool, please read the *Running the Intel® SCS System Discovery Utility* section on page 11.

The `FWVersion` value contains the version of firmware currently on the device. The `AMTSSKU` value contains the supported manageability SKU, if present. Review the values of `FWVersion` and `AMTSSKU` to determine your system's vulnerability as described in Table 6.

Table 6. Criteria to determine if a system is vulnerable to INTEL-SA-00075 using the Intel® SCS System Discovery Utility

Value Name	Vulnerable	Not Vulnerable
AMTSKU	Intel(R) Full AMT Manageability Intel(R) Standard Manageability Intel(R) Small Business Advantage(SBA) Example Output: <ManageabilityInfo> <AMTSKU>Intel(R) Full AMT Manageability</AMTSKU> <AMTversion>11.0.0</AMTversion> <FWVersion>11.0.0.1202</FWVersion>	AMTSKU value not present in the output -or- AMTSKU values to the left with a firmware version that is not vulnerable Example Output: <ManageabilityInfo> <FWVersion>9.0.13.1402</FWVersion>
FWVersion	Intel® manageability SKU firmware versions 6.x.x.x – 11.7.x.x with a build value less than 3000 Example: 9.5.22. 1760	Intel® manageability SKU firmware versions: <ul style="list-style-type: none"> • 6.x.x.x – 11.7.x.x with a build value greater or equal to 3000 <ul style="list-style-type: none"> ○ Example: 11.6.27.3264 • 2.x.x.x. – 5.x.x.x • 11.7.x.x or greater

Note: Intel® Small Business Technology (SBT) is the manageability SKU for Intel® Small Business Advantage (SBA).

Running the Intel® SCS System Discovery Utility

Saving data to the registry only

Run the following command from a command prompt with administrative rights to run Intel® System SCS Discovery Utility and write data to the registry:

```
SCSDiscovery.exe SystemDiscovery /nofile
```

Saving data to a XML file only

Use the following command to run Intel® SCS System Discovery Utility and save the data to an XML file:

```
SCSDiscovery.exe SystemDiscovery <filename and path> /noregistry
```

The file name and path can be a local location on the system or a network share. If you choose to use a network share, make sure the account running Intel® SCS System Discovery Utility has write permissions to that network share. If you don't specify a file name and path, the system's FQDN will be used for the XML file name and the file will be stored in the directory that contains the Intel® SCS System Discovery Utility.

Saving data to the registry and a XML file

Use the following command to run the Intel® SCS System Discovery Utility to save data to the registry and a XML file

```
SCSDiscovery.exe SystemDiscovery <filename and path>
```

As in the previous example, if you don't specify a file name and path, the system's FQDN will be used for the XML file name and the file will be stored in the directory that contains the Intel(R) SCS System Discovery Utility.

Results of the Intel® SCS System Discovery Utility

The amount of data returned by the Intel® SCS System Discovery Utility will depend on if the Intel manageability driver stack is loaded on to the system. If the Intel® Management Engine Interface (MEI) driver and Intel® Management and Security Application Local Management Service (LMS) are present, there will be a more verbose set of data available. The results described below will focus on just a few key data fields relevant to the known privilege escalation issue. For additional details on the other data fields, see the Intel® SCS System Discovery Utility documentation. Some of the fields may not be supported by the manufacturer.

Registry results

Results saved to the registry can be found in the following location:

```
HKLM\Software\Intel\Setup and Configuration Software\SystemDiscovery
```

Key values:

Value Name	Registry Sub key	Value Description
FWVersion	ManageabilityInfo	Intel® Management Engine firmware version
AMTSKU	ManageabilityInfo	Supported manageability feature, if any present

XML file results

The Intel® Management Engine firmware version is found in the following path in the XML:

```
<SystemDiscovery>
  <ManageabilityInfo>
    <FWVersion> Version Number </FWVersion>
```

The system's supported manageability feature, if present, is found in the following path in the XML:

```
<SystemDiscovery>
  <ManageabilityInfo>
    <AMTSKU> Manageability Feature Name </AMTSKU>
```

Importing system discovery data into SCCM hardware inventory

The process of collecting system discovery data can be automated with the Intel® SCS Add-on for Microsoft* System Center Configuration Manager (SCCM). When installed, this add-on will automatically extend the SCCM hardware inventory to include system discovery data as well as create task sequences that can be used to run system discovery against collections of systems. The information collected through this process can then be used to create SCCM collections to push firmware updates or mitigations to impacted systems.

The Intel® SCS Add-on for Microsoft SCCM download package is available at

<https://downloadcenter.intel.com/download/26506/Intel-SCS-Add-on-for-Microsoft-System-Center-Configuration-Manager>.

MOF file changes

```
//===== Intel-SA-00075 Start =====

#pragma namespace ("\\.\root\cimv2")
#pragma deleteclass("INTEL_SA_00075_DiscoveryTool", NOFAIL)
[DYNPROPS]
Class INTEL_SA_00075_DiscoveryTool
{
[key] string KeyName;
String ScanDate;
String ComputerName;
String ApplicationVersion;
};

[DYNPROPS]
Instance of INTEL_SA_00075_DiscoveryTool
{
[PropertyContext("Local|HKEY_LOCAL_MACHINE\SOFTWARE\Intel\Setup and Configuration
Software\INTEL-SA-00075 Discovery Tool|Scan Date"),Dynamic,Provider("RegPropProv")] ScanDate;
[PropertyContext("Local|HKEY_LOCAL_MACHINE\SOFTWARE\Intel\Setup and Configuration
Software\INTEL-SA-00075 Discovery Tool|Computer Name"),Dynamic,Provider("RegPropProv")]
ComputerName;
[PropertyContext("Local|HKEY_LOCAL_MACHINE\SOFTWARE\Intel\Setup and Configuration
Software\INTEL-SA-00075 Discovery Tool|Application Version"),Dynamic,Provider("RegPropProv")]
ApplicationVersion;
};

#pragma namespace ("\\.\root\cimv2")
#pragma deleteclass("INTEL_SA_00075_HardwareInventory", NOFAIL)
[DYNPROPS]
Class INTEL_SA_00075_HardwareInventory
{
[key] string KeyName;
String ComputerManufacturer;
String ComputerModel;
String Processor;
};

[DYNPROPS]
Instance of INTEL_SA_00075_HardwareInventory
{
[PropertyContext("Local|HKEY_LOCAL_MACHINE\SOFTWARE\Intel\Setup and Configuration
Software\INTEL-SA-00075 Discovery Tool\Hardware Inventory|Computer
Manufacturer"),Dynamic,Provider("RegPropProv")] ComputerManufacturer;
[PropertyContext("Local|HKEY_LOCAL_MACHINE\SOFTWARE\Intel\Setup and Configuration
Software\INTEL-SA-00075 Discovery Tool\Hardware Inventory|Computer
Model"),Dynamic,Provider("RegPropProv")] ComputerModel;
[PropertyContext("Local|HKEY_LOCAL_MACHINE\SOFTWARE\Intel\Setup and Configuration
Software\INTEL-SA-00075 Discovery Tool\Hardware
Inventory|Processor"),Dynamic,Provider("RegPropProv")] Processor;
};

#pragma namespace ("\\.\root\cimv2")
#pragma deleteclass("INTEL_SA_00075_MEFirmwareInformation", NOFAIL)
[DYNPROPS]
Class INTEL_SA_00075_MEFirmwareInformation
{
[key] string KeyName;
String MEVersion;
};
```

```
UInt32 MEVersionMajor;
UInt32 MEVersionMinor;
UInt32 MEVersionBuild;
UInt32 MEVersionHotfix;
String MESKU;
String MEProvisioningState;
String MEDriverInstalled;
String LMSState;
String MicroLMSState;
String EHBCPEnabled;
String IsCCMDisabled;
};

[DYNPROPS]
Instance of INTEL_SA_00075_MEFirmwareInformation
{
  [PropertyContext("Local|HKEY_LOCAL_MACHINE\\SOFTWARE\\Intel\\Setup and Configuration
Software\\INTEL-SA-00075 Discovery Tool\\ME Firmware Information|ME
Version"),Dynamic,Provider("RegPropProv")] MEVersion;
  [PropertyContext("Local|HKEY_LOCAL_MACHINE\\SOFTWARE\\Intel\\Setup and Configuration
Software\\INTEL-SA-00075 Discovery Tool\\ME Firmware Information|ME Version
Major"),Dynamic,Provider("RegPropProv")] MEVersionMajor;
  [PropertyContext("Local|HKEY_LOCAL_MACHINE\\SOFTWARE\\Intel\\Setup and Configuration
Software\\INTEL-SA-00075 Discovery Tool\\ME Firmware Information|ME Version
Minor"),Dynamic,Provider("RegPropProv")] MEVersionMinor;
  [PropertyContext("Local|HKEY_LOCAL_MACHINE\\SOFTWARE\\Intel\\Setup and Configuration
Software\\INTEL-SA-00075 Discovery Tool\\ME Firmware Information|ME Version
Build"),Dynamic,Provider("RegPropProv")] MEVersionBuild;
  [PropertyContext("Local|HKEY_LOCAL_MACHINE\\SOFTWARE\\Intel\\Setup and Configuration
Software\\INTEL-SA-00075 Discovery Tool\\ME Firmware Information|ME Version
Hotfix"),Dynamic,Provider("RegPropProv")] MEVersionHotfix;
  [PropertyContext("Local|HKEY_LOCAL_MACHINE\\SOFTWARE\\Intel\\Setup and Configuration
Software\\INTEL-SA-00075 Discovery Tool\\ME Firmware Information|ME
SKU"),Dynamic,Provider("RegPropProv")] MESKU;
  [PropertyContext("Local|HKEY_LOCAL_MACHINE\\SOFTWARE\\Intel\\Setup and Configuration
Software\\INTEL-SA-00075 Discovery Tool\\ME Firmware Information|ME Provisioning
State"),Dynamic,Provider("RegPropProv")] MEProvisioningState;
  [PropertyContext("Local|HKEY_LOCAL_MACHINE\\SOFTWARE\\Intel\\Setup and Configuration
Software\\INTEL-SA-00075 Discovery Tool\\ME Firmware Information|ME Driver
Installed"),Dynamic,Provider("RegPropProv")] MEDriverInstalled;
  [PropertyContext("Local|HKEY_LOCAL_MACHINE\\SOFTWARE\\Intel\\Setup and Configuration
Software\\INTEL-SA-00075 Discovery Tool\\ME Firmware Information|LMS
State"),Dynamic,Provider("RegPropProv")] LMSState;
  [PropertyContext("Local|HKEY_LOCAL_MACHINE\\SOFTWARE\\Intel\\Setup and Configuration
Software\\INTEL-SA-00075 Discovery Tool\\ME Firmware Information|Micro LMS
State"),Dynamic,Provider("RegPropProv")] MicroLMSState;
  [PropertyContext("Local|HKEY_LOCAL_MACHINE\\SOFTWARE\\Intel\\Setup and Configuration
Software\\INTEL-SA-00075 Discovery Tool\\ME Firmware Information|EHBCP
Enabled"),Dynamic,Provider("RegPropProv")] EHBCPEnabled;
  [PropertyContext("Local|HKEY_LOCAL_MACHINE\\SOFTWARE\\Intel\\Setup and Configuration
Software\\INTEL-SA-00075 Discovery Tool\\ME Firmware Information|Is CCM
Disabled"),Dynamic,Provider("RegPropProv")] IsCCMDisabled;
};

//===== Intel-SA-00075 End =====
```

INTEL-SA-00075.bat batch file

```
@echo off
.\Intel-SA-00075-console
SET EL=%ERRORLEVEL%
rem Schedule HW inventory
SET HWInventoryGUID="{00000000-0000-0000-0000-000000000001}"
wmic /IMPLEVEL:Impersonate /AUTHLEVEL:Pktprivacy /namespace:\\root\ccm path sms_client CALL
TriggerSchedule %HWInventoryGUID% /NOINTERACTIVE
echo Exit code: %EL%
exit %EL%
```

Collection query samples

Provisioned computers

```
select * from SMS_R_System inner join SMS_G_System_INTEL_SA_00075_MEFIRMWAREINFORMATION on
SMS_G_System_INTEL_SA_00075_MEFIRMWAREINFORMATION.ResourceId = SMS_R_System.ResourceId where
SMS_G_System_INTEL_SA_00075_MEFIRMWAREINFORMATION.MEProvisioningState = "Provisioned"
```

LMS running

```
select
SMS_R_SYSTEM.ResourceID,SMS_R_SYSTEM.ResourceType,SMS_R_SYSTEM.Name,SMS_R_SYSTEM.SMSUniqueIdentifie
r,SMS_R_SYSTEM.ResourceDomainORWorkgroup,SMS_R_SYSTEM.Client from SMS_R_System inner join
SMS_G_System_INTEL_SA_00075_MEFIRMWAREINFORMATION on
SMS_G_System_INTEL_SA_00075_MEFIRMWAREINFORMATION.ResourceID = SMS_R_System.ResourceId where
SMS_G_System_INTEL_SA_00075_MEFIRMWAREINFORMATION.LMSState = "Running" or
SMS_G_System_INTEL_SA_00075_MEFIRMWAREINFORMATION.MicroLMSState = "Running"
```

INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH INTEL® PRODUCTS. NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED BY THIS DOCUMENT. EXCEPT AS PROVIDED IN INTEL'S TERMS AND CONDITIONS OF SALE FOR SUCH PRODUCTS, INTEL ASSUMES NO LIABILITY WHATSOEVER, AND INTEL DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, RELATING TO SALE AND/OR USE OF INTEL PRODUCTS INCLUDING LIABILITY OR WARRANTIES RELATING TO FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR INFRINGEMENT OF ANY PATENT, COPYRIGHT OR OTHER INTELLECTUAL PROPERTY RIGHT. UNLESS OTHERWISE AGREED IN WRITING BY INTEL, THE INTEL PRODUCTS ARE NOT DESIGNED NOR INTENDED FOR ANY APPLICATION IN WHICH THE FAILURE OF THE INTEL PRODUCT COULD CREATE A SITUATION WHERE PERSONAL INJURY OR DEATH MAY OCCUR.

Intel technologies' features and benefits depend on system configuration and may require enabled hardware, software or service activation. Performance varies depending on system configuration. No computer system can be absolutely secure. Check with your system manufacturer or retailer or learn more at intel.com.

Copyright © 2017 Intel Corporation. All rights reserved. Intel and the Intel logo are trademarks of Intel Corporation in the U.S. and/or other countries.

* Other names and brands may be claimed as the property of others.