NIST SPECIAL PUBLICATION 1800-34C

Validating the Integrity of Computing Devices

Volume C:
How-To Guides

Tyler Diamond*
Nakia Grayson
William T. Polk
Andrew Regenscheid
Murugiah Souppaya
National Institute of Standards and Technology
Information Technology Laboratory

Christopher Brown
Chelsea Deane
The MITRE Corporation
McLean, Virginia

Karen Scarfone
Scarfone Cybersecurity
Clifton, Virginia

**Former employee; all work for this publication was done while at employer*

November 2021

PRELIMINARY DRAFT

This publication is available free of charge from
https://www.nccoe.nist.gov/projects/building-blocks/supply-chain-assurance

DISCLAIMER

Certain commercial entities, equipment, products, or materials may be identified by name or company logo or other insignia in order to acknowledge their participation in this collaboration or to describe an experimental procedure or concept adequately. Such identification is not intended to imply special status or relationship with NIST or recommendation or endorsement by NIST or NCCoE; neither is it intended to imply that the entities, equipment, products, or materials are necessarily the best available for the purpose.

While NIST and the NCCoE address goals of improving management of cybersecurity and privacy risk through outreach and application of standards and best practices, it is the stakeholder's responsibility to fully perform a risk assessment to include the current threat, vulnerabilities, likelihood of a compromise, and the impact should the threat be realized before adopting cybersecurity measures such as this recommendation.

National Institute of Standards and Technology Special Publication 1800-34C, Natl. Inst. Stand. Technol. Spec. Publ. 1800-34C, 116 pages, (November 2021), CODEN: NSPUE2

FEEDBACK

You can improve this guide by contributing feedback. As you review and adopt this solution for your own organization, we ask you and your colleagues to share your experience and advice with us.

Comments on this publication may be submitted to: supplychain-nccoe@nist.gov.

Public comment period: November 22, 2021 through January 17, 2022.

As a private-public partnership, we are always seeking feedback on our practice guides. We are particularly interested in seeing how businesses apply NCCoE reference designs in the real world. If you have implemented the reference design, or have questions about applying it in your environment, please email us at supplychain-nccoe@nist.gov.

All comments are subject to release under the Freedom of Information Act.

National Cybersecurity Center of Excellence
National Institute of Standards and Technology
100 Bureau Drive
Mailstop 2002
Gaithersburg, MD 20899
Email: nccoe@nist.gov

NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

The National Cybersecurity Center of Excellence (NCCoE), a part of the National Institute of Standards and Technology (NIST), is a collaborative hub where industry organizations, government agencies, and academic institutions work together to address businesses' most pressing cybersecurity issues. This public-private partnership enables the creation of practical cybersecurity solutions for specific industries, as well as for broad, cross-sector technology challenges. Through consortia under Cooperative Research and Development Agreements (CRADAs), including technology partners—from Fortune 50 market leaders to smaller companies specializing in information technology security—the NCCoE applies standards and best practices to develop modular, adaptable example cybersecurity solutions using commercially available technology. The NCCoE documents these example solutions in the NIST Special Publication 1800 series, which maps capabilities to the NIST Cybersecurity Framework and details the steps needed for another entity to re-create the example solution. The NCCoE was established in 2012 by NIST in partnership with the State of Maryland and Montgomery County, Maryland.

To learn more about the NCCoE, visit https://www.nccoe.nist.gov/. To learn more about NIST, visit https://www.nist.gov.

NIST CYBERSECURITY PRACTICE GUIDES

NIST Cybersecurity Practice Guides (Special Publication 1800 series) target specific cybersecurity challenges in the public and private sectors. They are practical, user-friendly guides that facilitate the adoption of standards-based approaches to cybersecurity. They show members of the information security community how to implement example solutions that help them align with relevant standards and best practices, and provide users with the materials lists, configuration files, and other information they need to implement a similar approach.

The documents in this series describe example implementations of cybersecurity practices that businesses and other organizations may voluntarily adopt. These documents do not describe regulations or mandatory practices, nor do they carry statutory authority.

ABSTRACT

Organizations are increasingly at risk of cyber supply chain compromise, whether intentional or unintentional. Cyber supply chain risks include counterfeiting, unauthorized production, tampering, theft, and insertion of unexpected software and hardware. Managing these risks requires ensuring the integrity of the cyber supply chain and its products and services. This project will demonstrate how organizations can verify that the internal components of the computing devices they acquire, whether laptops or servers, are genuine and have not been tampered with. This solution relies on device vendors storing information within each device, and organizations using a combination of commercial off-the-shelf and open-source tools that work together to validate the stored information. This NIST

Cybersecurity Practice Guide provides a preliminary draft describing the work performed so far to build and test the full solution.

KEYWORDS

computing devices; cyber supply chain; cyber supply chain risk management (C-SCRM); hardware root of trust; integrity; provenance; supply chain; tampering.

ACKNOWLEDGMENTS

We are grateful to the following individuals for their generous contributions of expertise and time.

Name	Organization
Charles Robison	Dell Technologies
Mukund Khatri	Dell Technologies
Rick Martinez	Dell Technologies
Daniel Carroll	Dell Technologies
Travis Raines	Eclypsium
John Loucaides	Eclypsium
Jason Cohen	Hewlett Packard Enterprise
CJ Coppersmith	Hewlett Packard Enterprise
Boris Balacheff	HP Inc.
Jeff Jeansonne	HP Inc.
Joshua Schiffman	HP Inc.
Tom Dodson	Intel
Jason Ajmo	The MITRE Corporation

Name	Organization
Chelsea Deane	The MITRE Corporation
Spike E. Dog	The MITRE Corporation
Joe Sain	The MITRE Corporation
Thomas Walters	The MITRE Corporation
Andrew Medak	National Security Agency (NSA)
Lawrence Reinert	NSA
Themistocles Chronis	RSA
Dan Carayiannis	RSA
Manuel Offenberg	Seagate
David Kaiser	Seagate
Paul Gatten	Seagate
Simon Phatigaraphong	Seagate
Bill Downer	Seagate Government Solutions
Jack Fabian	Seagate Government Solutions

The Technology Partners/Collaborators who participated in this build submitted their capabilities in response to a notice in the Federal Register. Respondents with relevant capabilities or product components were invited to sign a Cooperative Research and Development Agreement (CRADA) with NIST, allowing them to participate in a consortium to build this example solution. We worked with:

Technology Partner/Collaborator	Build Involvement
Dell Technologies	PowerEdge R650, Secured Component Verification tool; Precision 3530, CSG Secured Component Verification tool
Eclypsium	Eclypsium Analytics Service, Eclypsium Device Scanner
HP Inc.	(2) Elitebook 840 G7, HP Sure Start, HP Sure Recover, Sure Admin, HP Client Management Script Library (CMSL), HP Tamperlock
Hewlett Packard Enterprise	Proliant DL360
Intel	HP Inc. Elitebook 360 830 G5, Lenovo ThinkPad T480, Transparent Supply Chain Tools, Key Generation Facility, Cloud Based Storage, TSCVerify and AutoVerify software tools
National Security Agency (NSA)	Host Integrity at Runtime and Start-Up (HIRS), Subject Matter Expertise
RSA	RSA Archer Suite 6.9
Seagate Government Solutions	(3) 18TB Exos X18 hard drives, Firmware Attestation API, Secure Device Authentication API

DOCUMENT CONVENTIONS

The terms “shall” and “shall not” indicate requirements to be followed strictly to conform to the publication and from which no deviation is permitted. The terms “should” and “should not” indicate that among several possibilities, one is recommended as particularly suitable without mentioning or excluding others, or that a certain course of action is preferred but not necessarily required, or that (in the negative form) a certain possibility or course of action is discouraged but not prohibited. The terms “may” and “need not” indicate a course of action permissible within the limits of the publication. The terms “can” and “cannot” indicate a possibility and capability, whether material, physical, or causal.

CALL FOR PATENT CLAIMS

This public review includes a call for information on essential patent claims (claims whose use would be required for compliance with the guidance or requirements in this Information Technology Laboratory (ITL) draft publication). Such guidance and/or requirements may be directly stated in this ITL Publication or by reference to another publication. This call also includes disclosure, where known, of the existence of pending U.S. or foreign patent applications relating to this ITL draft publication and of any relevant unexpired U.S. or foreign patents.

ITL may require from the patent holder, or a party authorized to make assurances on its behalf, in written or electronic form, either:

a) assurance in the form of a general disclaimer to the effect that such party does not hold and does not currently intend holding any essential patent claim(s); or

b) assurance that a license to such essential patent claim(s) will be made available to applicants desiring to utilize the license for the purpose of complying with the guidance or requirements in this ITL draft publication either:

1. under reasonable terms and conditions that are demonstrably free of any unfair discrimination; or
2. without compensation and under reasonable terms and conditions that are demonstrably free of any unfair discrimination.

Such assurance shall indicate that the patent holder (or third party authorized to make assurances on its behalf) will include in any documents transferring ownership of patents subject to the assurance, provisions sufficient to ensure that the commitments in the assurance are binding on the transferee, and that the transferee will similarly include appropriate provisions in the event of future transfers with the goal of binding each successor-in-interest.

The assurance shall also indicate that it is intended to be binding on successors-in-interest regardless of whether such provisions are included in the relevant transfer documents.

Such statements should be addressed to: supplychain-nccoe@nist.gov

Contents

List of Figures

List of Tables

1 Introduction

The following volumes of this guide show information technology (IT) professionals and security engineers how we implemented this example solution. We cover all of the products employed in this reference design. We do not re-create the product manufacturers' documentation, which is presumed to be widely available. Rather, these volumes show how we incorporated the products together in our environment.

Note: These are not comprehensive tutorials. There are many possible service and security configurations for these products that are out of scope for this reference design.

1.1 How to Use This Guide

This National Institute of Standards and Technology (NIST) Cybersecurity Practice Guide demonstrates a standards-based reference design and provides users with the information they need to replicate verifying that the internal components of the computing devices they acquire are genuine and have not been tampered with. This reference design is modular and can be deployed in whole or in part.

This guide contains three volumes:

- NIST Special Publication (SP) 1800-34A: *Executive Summary*
- NIST SP 1800-34B: *Approach, Architecture, and Security Characteristics* – what we built and why
- NIST SP 1800-34C: *How-To Guides* – instructions for building the example solution **(you are here)**

Depending on your role in your organization, you might use this guide in different ways:

Business decision makers, including chief security and technology officers, will be interested in the *Executive Summary, NIST SP 1800-34A*, which describes the following topics:

- challenges that enterprises face in decreasing the risk of a compromise to products in their supply chain
- example solution built at the NCCoE
- benefits of adopting the example solution

Technology or security program managers who are concerned with how to identify, understand, assess, and mitigate risk will be interested in *NIST SP 1800-34B*, which describes what we did and why. The following sections will be of particular interest:

- Section 3.4, Risk, describes the risk analysis we performed.
- Section 3.5, Security Control Map, maps the security characteristics of this example solution to cybersecurity standards and best practices.

You might share the *Executive Summary, NIST SP 1800-34A*, with your leadership team members to help them understand the importance of adopting a standards-based solution for verifying that the internal components of the computing devices they acquire are genuine and have not been tampered with.

IT professionals who want to implement an approach like this will find this whole practice guide useful. You can use this How-To portion of the guide, *NIST SP 1800-34C*, to replicate all or parts of the build created in our lab. This How-To portion of the guide provides specific product installation, configuration, and integration instructions for implementing the example solution.

This guide assumes that IT professionals have experience implementing security products within the enterprise. While we have used a suite of commercial products to address this challenge, this guide does not endorse these particular products. Your organization can adopt this solution or one that adheres to these guidelines in whole, or you can use this guide as a starting point for tailoring and implementing parts of verifying that the internal components of the computing devices they acquire are genuine and have not been tampered with. Your organization's security experts should identify the products that will best integrate with your existing tools and IT system infrastructure. We hope that you will seek products that are congruent with applicable standards and best practices. Section 3.6, Technologies, of *NIST SP 1800-34B* lists the products that we used and maps them to the cybersecurity controls provided by this reference solution.

A NIST Cybersecurity Practice Guide does not describe "the" solution, but a possible solution. This is a preliminary draft guide. We seek feedback on its contents and welcome your input. Comments, suggestions, and success stories will improve subsequent versions of this guide. Please contribute your thoughts to supplychain-nccoe@nist.gov.

1.1.1 Supplemental Material

Throughout this preliminary draft there are references to code, scripts, and/or configuration files. Due to the size of some of the files, and to provide a more efficient method of access, in a future update we will make these assets available via a NIST GitHub repository. This will also enable quicker updates of published code to those interested in replicating our demonstration.

1.2 Build Overview

This preliminary draft of Volume C describes the steps necessary to set up an environment that focuses on laptop (sometimes referred to by industry as *client*) computing devices. It also provides guidance on the operational usage of manufacturers' tools that may be useful to your IT personnel who verify that the computing device is acceptable to receive into the acquiring organization. In a future draft of Volume C, we will incorporate validating the integrity of servers and include additional enterprise services as required to support this capability.

1.3 Typographic Conventions

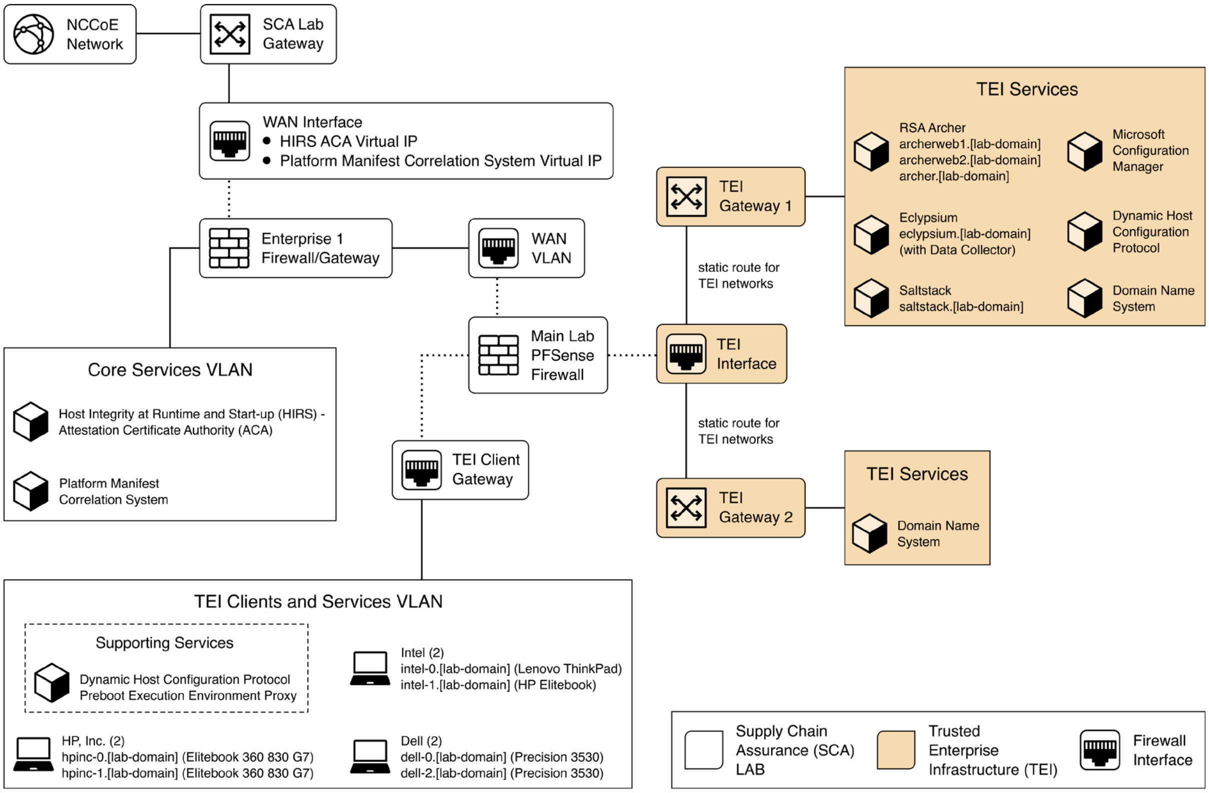
The following table presents typographic conventions used in this volume.

Typeface/Symbol	Meaning	Example
Italics	file names and path names; references to documents that are not hyperlinks; new terms; and placeholders	For language use and style guidance, see the *NCCoE Style Guide*.
Bold	names of menus, options, command buttons, and fields	Choose **File** > **Edit.**
`Monospace`	command-line input, onscreen computer output, sample code examples, and status codes	`mkdir`
`Monospace Bold`	command-line user input contrasted with computer output	**`service sshd start`**
blue text	link to other parts of the document, a web URL, or an email address	All publications from NIST's NCCoE are available at https://www.nccoe.nist.gov.

1.4 Logical Architecture Summary

Figure 1-1 depicts the work-in-progress architecture for the prototype demonstration environment used within the NCCoE network boundaries. The environment uses a combination of physical and virtual systems to emulate an enterprise architecture. Common enterprise services, such as Active Directory (AD) and Domain Name System (DNS), are provided by NCCoE's Trusted Enterprise Infrastructure (TEI). TEI provides common services that labs can use. Previously each lab would spend time and resources to set up common services at the beginning of each project and tear them down after the end of the project. To provide efficiency and consistency across projects, and to represent a true enterprise infrastructure, NCCoE has initiated the TEI effort, which offers common services such as core services and shared security services for those labs who would like to use them.

Figure 1-1 Laptop Build Architecture


NCCoE Network
SCA Lab Gateway
WAN Interface
HIRS ACA Virtual IP
Platform Manifest Correlation System Virtual IP
Enterprise 1 Firewall/Gateway
WAN VLAN
Main Lab PFSense Firewall
Core Services VLAN
Host Integrity at Runtime and Start-up (HIRS) - Attestation Certificate Authority (ACA)
Platform Manifest Correlation System
TEI Client Gateway
TEI Gateway 1
static route for TEI networks
TEI Interface
static route for TEI networks
TEI Gateway 2
TEI Services
RSA Archer
archerweb1.[lab-domain]
archerweb2.[lab-domain]
archer.[lab-domain]
Microsoft Configuration Manager
Eclypsium
eclypsium.[lab-domain]
(with Data Collector)
Dynamic Host Configuration Protocol
Saltstack
saltstack.[lab-domain]
Domain Name System
TEI Services
Domain Name System
TEI Clients and Services VLAN
Supporting Services
Dynamic Host Configuration Protocol Preboot Execution Environment Proxy
Intel (2)
intel-0.[lab-domain] (Lenovo ThinkPad)
intel-1.[lab-domain] (HP Elitebook)
HP, Inc. (2)
hpinc-0.[lab-domain] (Elitebook 360 830 G7)
hpinc-1.[lab-domain] (Elitebook 360 830 G7)
Dell (2)
dell-0.[lab-domain] (Precision 3530)
dell-2.[lab-domain] (Precision 3530)
Supply Chain Assurance (SCA) LAB
Trusted Enterprise Infrastructure (TEI)
Firewall Interface

Services specific to the capabilities of this prototype demonstration are instantiated on the Core Services virtual network. This virtual network represents the integration of supply chain risk management (SCRM) requirements into an enterprise architecture to support the SCRM controls, as described in the Risk Assessment section of Volume B.

2 Product Installation Guides

This section of the practice guide contains detailed instructions for installing and configuring all of the products used to build an instance of the example solution.

2.1 Supporting Systems and Infrastructure

This section describes the supporting infrastructure required to execute the acceptance testing and continuous monitoring capabilities provided by our collaborators.

2.1.1 Network Boot Services

The following procedures will create an environment that will enable the acceptance testing of computing devices into an enterprise. First, we create a CentOS7 and WinPE images that will be booted on computing devices via a Preboot Execution Environment (PXE). We then configure the PXE environment to boot the images.

2.1.1.1 Linux-Based Acceptance Testing Image Creation

On a development CentOS7 system, install the latest version of the HIRS TPM Provisioner. We'll use the system as a basis to create the network booted image. Note that there are a number of dependencies that you'll need to satisfy before installing the Host Integrity at Runtime and Start-Up (HIRS) Trusted Platform Module (TPM) Provisioner package. One of those dependencies, PACCOR, is maintained by the HIRS project. In our prototype demonstration, we used version 1.1.4 revision 5 but recommend using the latest version available. Note that any version prior to revision 5 will not successfully complete the provisioning process with the laptop computing devices used in this demonstration.

2.1.1.1.1 HIRS Provisioner Configuration

The HIRS TPM provisioner is the core application in the computing device acceptance testing process. The system running the provisioner must be configured for your local environment before use.

1. Use a text editor to configure the HIRS Provisioner for your local environment.

   ```
   $ [your favorite editor] /etc/hirs/hirs-site.config
   ```

2. Change the variables noted below and save the file.

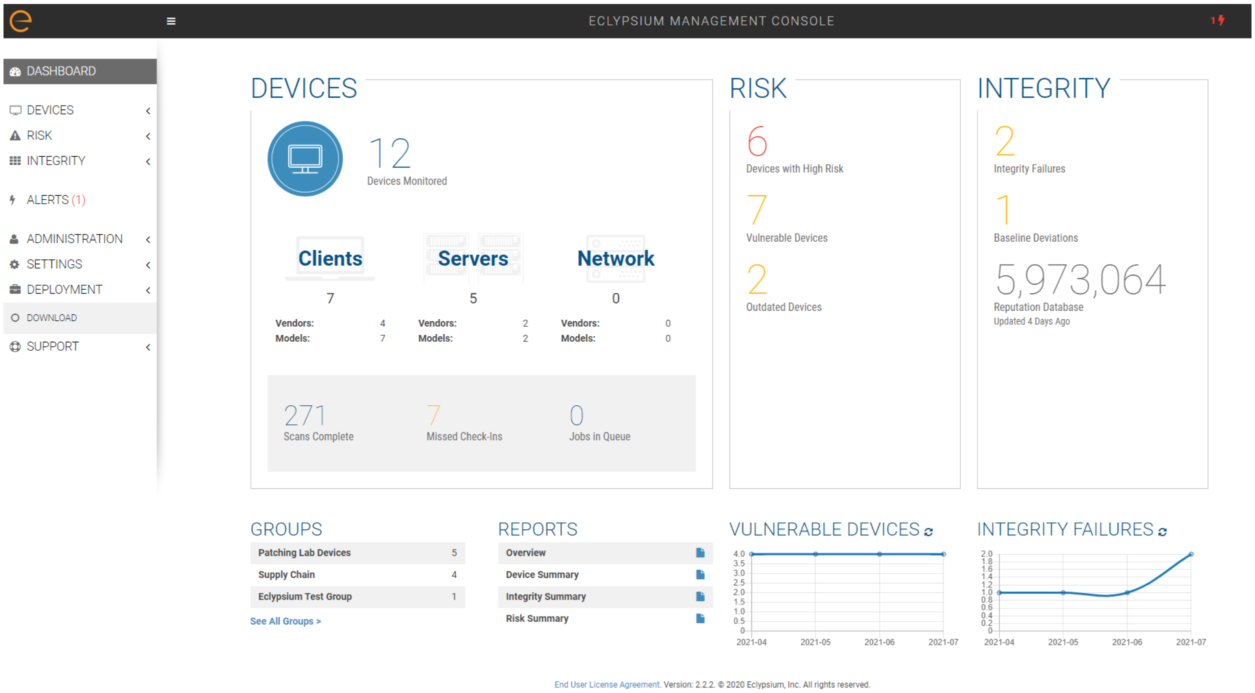
   ```
   #********************************************
   #* HIRS site configuration properties file
   #********************************************

   # Client configuration
   CLIENT_HOSTNAME=localhost
   TPM_ENABLED=true
   IMA_ENABLED=false

   # Site-specific configuration
   ATTESTATION_CA_FQDN=hirs-server.yourdomain.test
   ATTESTATION_CA_PORT=8443
   BROKER_FQDN=hirs-server.yourdomain.test
   # Change this port number to your local configuration
   BROKER_PORT=61616
   PORTAL_FQDN=hirs-server.yourdomain.test
   # Change this port number to your local configuration
   PORTAL_PORT=8443
   ```

3. If using a network boot environment, use the configuration file (step 2) in the kickstart file that creates the Centos7 provisioner image in the `%post` section.

2.1.1.1.2 Eclypsium Agent Configuration

On the same Centos7 system described in Section 2.1.1.1.1, install the Eclypsium Linux agent using the following procedures.

1. Navigate to the **Eclypsium Management Console** in a web browser.



GROUPS	
Patching Lab Devices	5
Supply Chain	4
Eclypsium Test Group	1

See All Groups >

REPORTS
Overview
Device Summary
Integrity Summary
Risk Summary

End User License Agreement. Version: 2.2.2. © 2020 Eclypsium, Inc. All rights reserved.

2. Select **Deployment** > **Download**.
3. Download the Linux (RPM) Portable Scanner. The filename will have the format `eclypsium_agent_builder-x.x.x.run`.
4. Install the prerequisites for the builder script.

   ```
   # yum groupinstall "Development Tools"
   ```

   ```
   # yum install kernel-devel
   ```

5. Run the builder script downloaded above as a user with root privileges. This will build the Eclypsium Portable Scanner drivers, extract the application binaries, and place them into a directory named `eclypsium_agent`.

   ```
   # ./eclypsium_agent_builder-X.X.X.run -out [PATH]
   ```

6. Confirm the previous step was successful by listing the `eclypsium_agent` directory and ensuring the portable scanner was created with the name `EclypsiumAppPortable`. This executable is referenced by our customized acceptance testing script.

2.1.1.1.3 CentOS 7 Image Creation

The CentOS 7 image we created enables quick revisions and simultaneous measurements on our devices. The image runs the required kernel, configures the system for reaching our infrastructure, and includes vendor tools to perform platform measurements. In order to generate the CentOS 7 image, the livecd-creator tool is utilized on a separate CentOS 7-based system. This tool uses Anaconda, Kickstart, and Lorax to generate the image. The following steps are performed:

1. Install the latest *livecd-tools* package, preferably built directly from the project GitHub repository.
2. Create your own kickstart file or use the kickstart that will be provided by this project as a basis. In our kickstart, we will insert commands to install required dependencies of our vendor products. Your environment will require further configuration to include networking, host file modification, and user management. You will also need to adjust hostnames and IP addresses to fit your environment.
3. Some tools, such as required drivers, were installed into a local repository (repo) on the image generating system using the *createrepo* command. This repo can be accessed by kickstart during the image generation. Copy *HIRS_Provisioner_TPM_2_0-X.X.X.x86_64.rpm* and *paccor-X.X.X-X.noarch.rpm* into the newly created repository.

```
$ createrepo -u file:///sca-packages sca-packages
```

4. Generate the ISO image from the kickstart file.

```
$ livecd-creator --config=kickstart-filename.ks
```

5. The ISO file will be created in the local directory with a filename indicating the time of generation. Once this is done, the *pxeboot* directory can be generated:

```
$ livecd-iso-to-pxeboot imagename.iso
```

6. The *pxeboot* directory will be created, containing the required *vmlinuz* and *initrd0.img* files. It will also create a directory name *pxelinux.cfg* which contains a file named *default*. *default* contains the kernel flags necessary to boot the image. Use these files in the PXE environment detailed in Section 2.1.1.3.

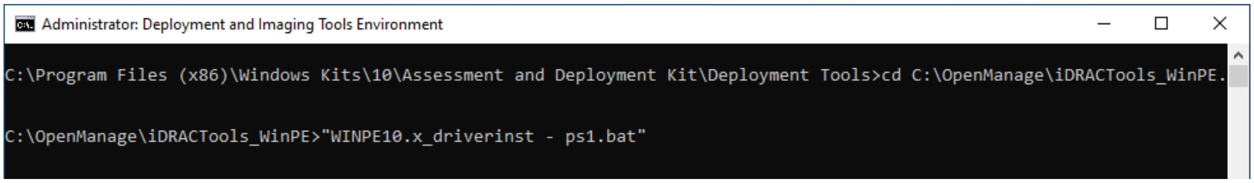
2.1.1.2 Windows-Based Acceptance Testing Image Creation

The following procedures will produce a WinPE bootable image that can be used in computing device acceptance testing. You will need to have a Windows Server (2016 or above) environment available to complete the following steps.

2.1.1.2.1 Build WinPE

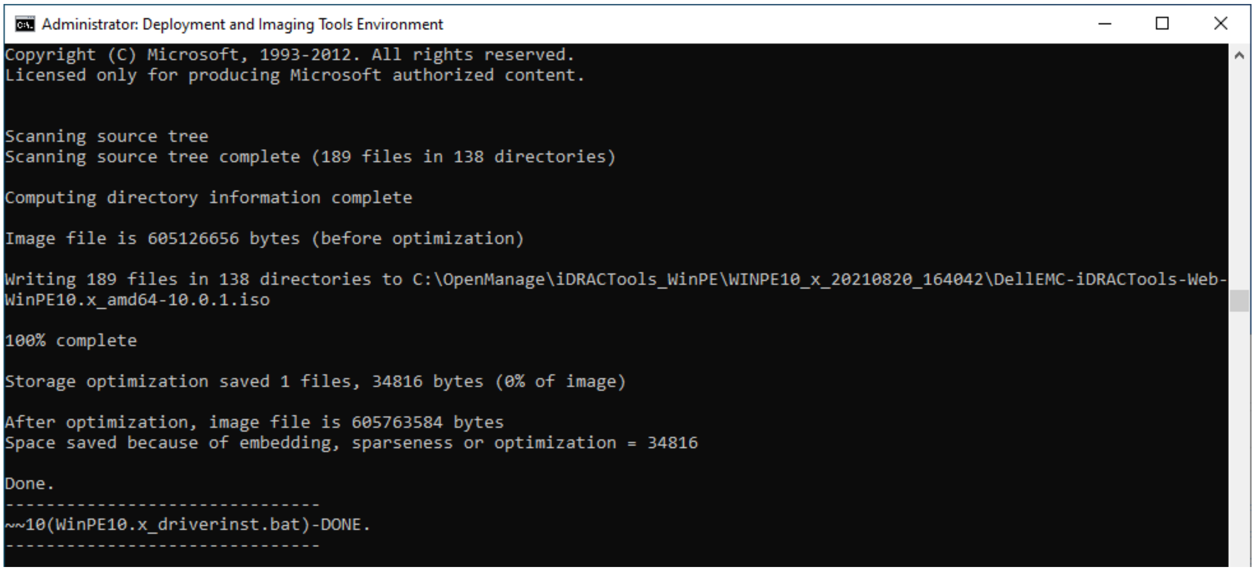
1. Download and install the Windows Assessment and Deployment Kit (ADK) and WinPE add-on.

2. Download the Dell EMC iDRAC Tools for Microsoft WinPE (R), v10.1.0.0 software package.
3. Run the self-extractor and choose all defaults.
4. Launch *cmd.exe* as an administrator and change directory to the extracted folder, then run our modified batch file (`WinPE10.x_driverinst - ps1.bat`).



```
C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit\Deployment Tools>cd C:\OpenManage\iDRACTools_WinPE.

C:\OpenManage\iDRACTools_WinPE>"WINPE10.x_driverinst - ps1.bat"
```

5. If successful, the preceding batch script will create a folder in the same directory with a name similar to *WINPE10.x-%timestamp%* or *WINPE5.x-%timestamp%*.



```
Copyright (C) Microsoft, 1993-2012. All rights reserved.
Licensed only for producing Microsoft authorized content.


Scanning source tree
Scanning source tree complete (189 files in 138 directories)

Computing directory information complete

Image file is 605126656 bytes (before optimization)

Writing 189 files in 138 directories to C:\OpenManage\iDRACTools_WinPE\WINPE10_x_20210820_164042\DellEMC-iDRACTools-Web-
WinPE10.x_amd64-10.0.1.iso

100% complete

Storage optimization saved 1 files, 34816 bytes (0% of image)

After optimization, image file is 605763584 bytes
Space saved because of embedding, sparseness or optimization = 34816

Done.
-------------------------------
~~10(WinPE10.x_driverinst.bat)-DONE.
-------------------------------
```

2.1.1.3 Preboot Execution Environment (PXE)

2.1.1.3.1 Dynamic Host Configuration Protocol (DHCP) Proxy

In this prototype demonstration, we use a combination of DNSMasq and the iPXE project to deliver the acceptance testing capabilities to computing devices. DNSMasq provides network boot services via DHCP on a network that already has other DHCP services present, such as assigning IP addresses to hosts. Since our network used DHCP services that could not easily be modified for network boot, we made the design decision to use DNSMasq as a proxy. However, for your setup you may want to include network boot services directly into the DHCP product that is used in your environment.

The iPXE project provides open-source network boot firmware. Using iPXE enabled a script-based boot process from an HTTP server. We also chainload the iPXE boot process from a Trivial File Transfer Protocol (TFTP) server, avoiding the need to replace the network card firmware with an iPXE client.

The system specification and procedures follow below. Note that this project uses computing devices that support Unified Extensible Firmware Interface (UEFI) booting and does not support legacy PC BIOS booting. Table 2-1 shows the system information used in our prototype demonstration.

Table 2-1 DHCP Proxy System Information

Operating System	Version	Platform
Ubuntu Server	Release 20.04	Virtual Machine

1. Install DNSMasq, the TFTP server, and the HTTP server using the software package manager of your chosen operating system (OS). On Ubuntu, use the following command.

   ```
   $ apt install dnsmasq tftpd-hpa apache2
   ```

2. Create a custom iPXE bootloader that directs iPXE to boot from a fixed URL.

   a. Create a file named *embed.ipxe* with the following contents.

      ```
      #!ipxe

      dhcp
      chain http://<IP or Hostname>/ipxe/boot.ipxe || shell
      ```

   b. Download and extract the iPXE source files. Install all software dependencies noted on the download page.

   c. Change directory to *ipxe/src* and run the following command.

      ```
      $ make bin-x86_64-efi/ipxe.efi EMBED=/path/to/embed.ipxe
      ```

3. Copy the newly built iPXE efi boot file to */var/lib/tftpboot*.

4. Edit the DNSMasq configuration file to suit your environment.

   a.
      ```
      $ [your favorite editor] /etc/dnsmasq.conf
      ```

   b. Ensure the following configuration variables are set in the configuration file:

      ```
      pxe-service=x86-64_efi,"Network Boot EFI",ipxe.efi
      enable-tftp
      tftp-root=/var/lib/tftpboot
      ```

5. Restart DNSMasq.

   ```
   $ systemctl restart dnsmasq
   ```

6. Copy the WinPE and CentOS7 images to the HTTP server.
    a. In the root of your HTTP server, create two directories to store the images.

    ```
    $ mkdir -p images/winpe images/centos7
    ```

    b. Copy the */media* directory created in Section 2.1.1.2.1 to *images/winpe*.
    c. Copy *initrd.img* and *vmlinuz* created in Section 2.1.1.1.2 to *images/centos7*.
    d. Download the latest wimboot binary from the iPXE repository and store it in the *images* directory.
7. Create a directory named *ipxe* in the HTTP server root, and copy the *boot.ipxe* file supplied by this project's repository to this location. Consider our configuration file as a starting point and ensure the contents of this file match your environment. Errors may result in a non-functioning network boot service.

2.1.2 Platform Manifest Correlation System (PMCS)

The PMCS is custom software that allows original equipment manufacturer (OEM) platform manifests (post-acceptance testing) to be translated into a format that is suitable for the Asset Discovery and Repository System (RSA Archer). The system provides a web UI for the IT administrator, and representational state transfer (REST) application programming interfaces (APIs) are provided for programmatic access. The following steps will set up the environment.

1. The system is based on Node.js, an open-source JavaScript runtime built on Chrome's V8 JavaScript engine designed to build scalable network applications. Download and install Node.js on a system best suited for your environment. This demonstration uses an Ubuntu 20.04.2 LTS virtual machine.
2. Install the node package manager (npm).
3. Install git on the platform chosen in Step 1. Git provides source code management capabilities used in later steps.
4. Install Process Manager 2 (PM2). This package will manage the Node.js processes that run the PMCS codebase.

    ```
    $ npm install pm2 -g
    ```

5. Clone the PMCS codebase via *git*.

    ```
    $ git clone https://<repository-hostname>/hrot/archer-api.git
    ```

6. Start the application using *pm2*.

    ```
    $ cd archer-api
    ```

```
$ pm2 start index.js
```

The PMCS should now be running as a background process. Consider using a startup script to keep your process list intact across expected or unexpected machine restarts.

2.2 Dell

Perform the following preparatory steps to create an acceptance testing environment suitable for Dell laptops. Contact your Dell representative to retrieve the proof-of-concept scripts referenced below.

1. Create a Platform Attribute Certificate for a target Dell laptop by first renaming the Dell script package from *{package_name}.zi_* to *{package_name}.zip*.
2. On the target computing device, unzip the contents of the zip file to the root directory (e.g., *C:\*)
3. Open a command prompt with administrative privileges.
4. Run *Gen_Plat_Cert.bat*. The Platform Attribute Certificate will be located at *o:\EFI\tcg\cert\platform* and at *.\{unzipped folder}\paccor\scripts\pc_testgen*.
5. Create a dedicated CentOS7 host for running the HIRS ACA portal that is accessible to the computing device undergoing acceptance testing. This step is detailed in Section 2.4.
6. Create a network bootable CentOS7 image. This step is detailed in Section 2.1.1.

2.3 Eclypsium

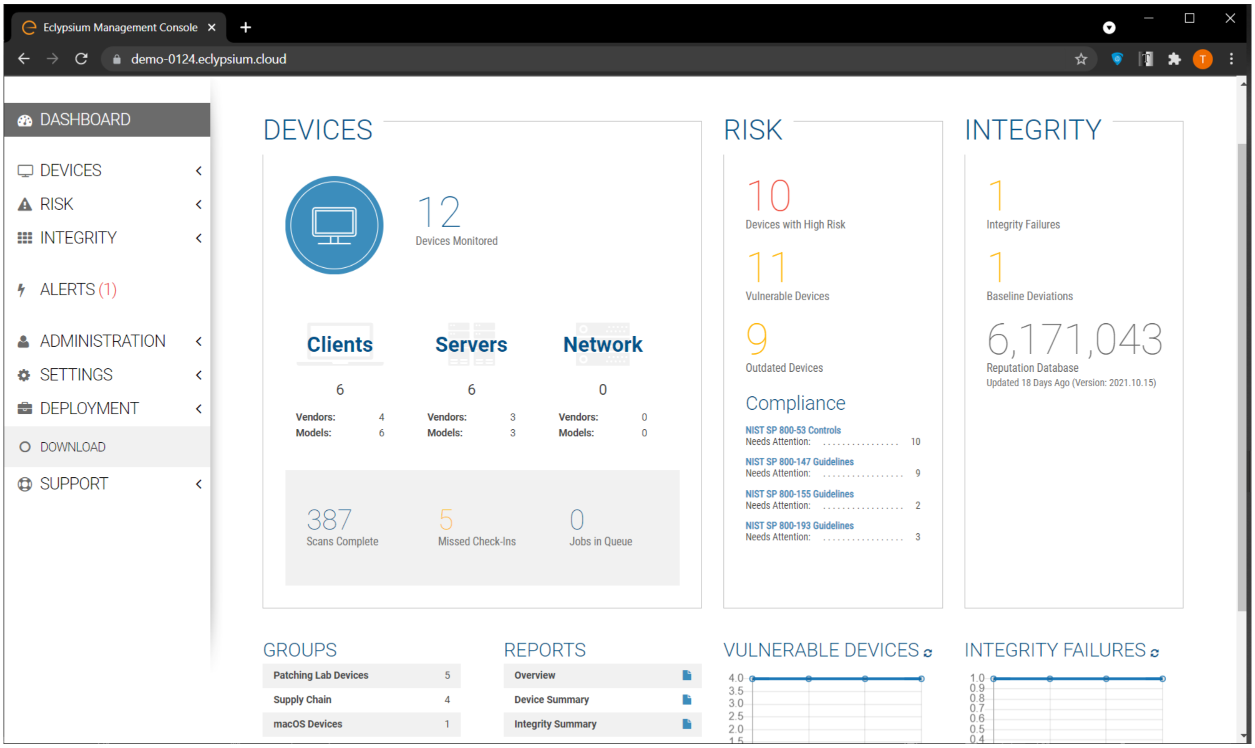
Eclypsium is a cloud-based firmware security solution. It secures firmware in servers, endpoints, and network devices by:

- identifying devices that contain firmware and creating detailed profiles of each component;
- verifying these profiles are free of vulnerabilities, have maintained their integrity, and are properly configured; and
- fortifying device firmware through a combination of configuration hardening, automated updates, and packaged guidance.

For this demonstration, Eclypsium is leveraged in the acceptance testing and continuous monitoring scenarios. The procedures below will install the Eclypsium agent and continuously monitor Windows-based laptops.

2.3.1 Download Eclypsium Agent

1. Navigate to the **Eclypsium Management Console** in a web browser.



2. Select **Deployment** > **Download**.

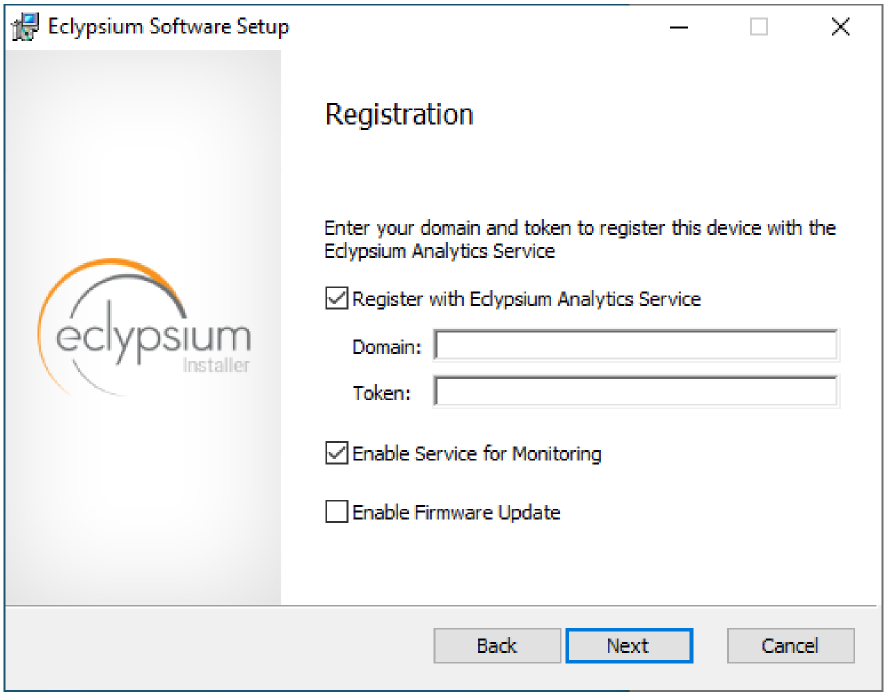
3. Download the installer for the appropriate OS (Windows, macOS, Linux (Deb), or Linux (RPM).

2.3.2 Install Eclypsium Agent for Windows

1. Start the Eclypsium bundled installer, *Eclypsium-2.8.1.exe*.

2. Select **Next**.

3. Ensure **Register with Eclypsium Analytics Service** and **Enable Service for Monitoring** are selected. Enter the **Domain** and Registration **Token** that can be found on the Download page of the **Eclypsium Management Console**, then select **Next.**



Registration

Enter your domain and token to register this device with the Eclypsium Analytics Service

☑ Register with Eclypsium Analytics Service

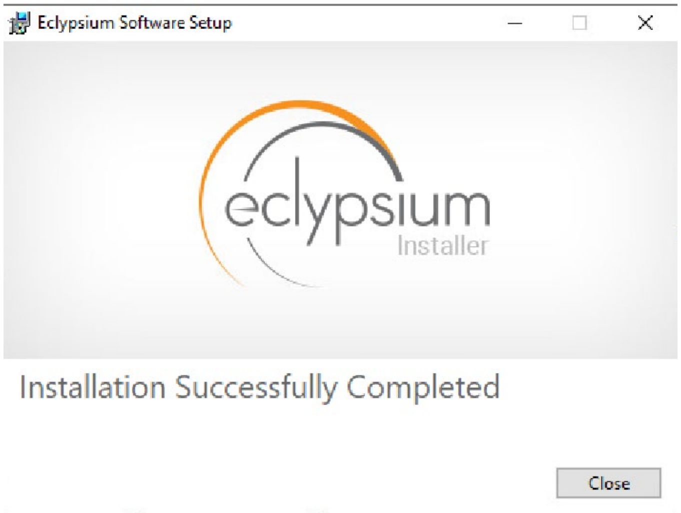
Domain:

Token:

☑ Enable Service for Monitoring

□ Enable Firmware Update

4. Select **Install** to start the Eclypsium installation**.**
5. When prompted, select **Finish.**
6. The Eclypsium agent has successfully installed once the page depicted below is reached. Select **Close.**



Installation Successfully Completed

When the system scan completes on a newly installed system, the Eclypsium console will identify supply chain integrity concerns and recommend a resolution.

2.4 Host Integrity at Runtime and Start-Up (HIRS) Attestation Certificate Authority (ACA)

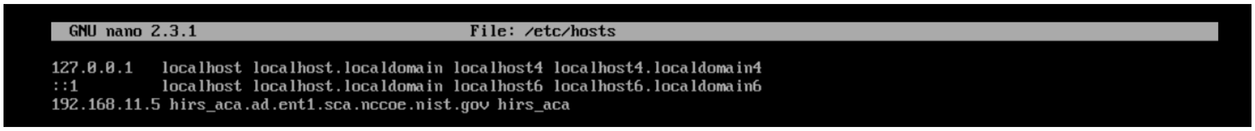
This section describes the installation and configuration of the HIRS-ACA backend components used in the acceptance testing scenario. HIRS-ACA is an open-source tool with three components that are used in this demonstration – the Attestation Certificate Authority, dashboard, and provisioner. The ACA issues identity credentials to devices that have a TPM 2.0 security module; these credentials are requested by the provisioner software. The HIRS-ACA dashboard is available to administrators to view and configure validation reports, credentials, and certificate trust chains. Table 2-2 shows the system information used in our prototype demonstration.

Table 2-2 HIRS-ACA System Information

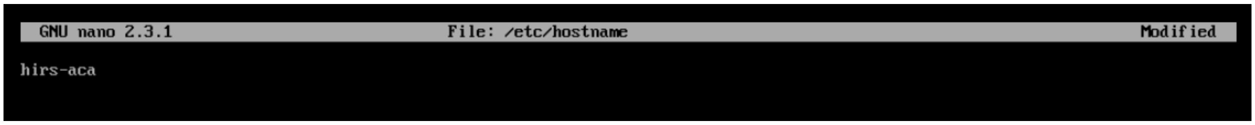
Operating System	Version	Platform
Centos	7	Virtual Machine

2.4.1 Installing the HIRS-ACA

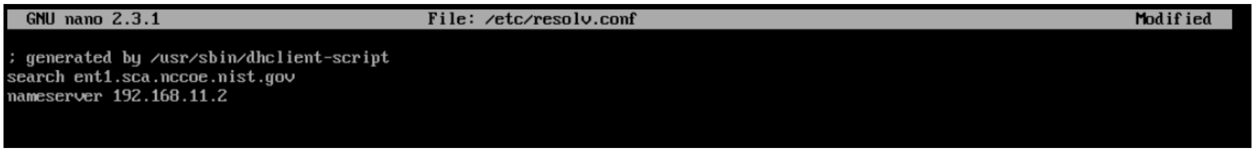
1. Before installing the required packages, ensure the target system has a fully qualified distinguished hostname. Modify the */etc/hosts*, */etc/hostname*, and */etc/resolv.conf* system configuration files as appropriate.



```
  GNU nano 2.3.1                             File: /etc/hosts

127.0.0.1   localhost localhost.localdomain localhost4 localhost4.localdomain4
::1         localhost localhost.localdomain localhost6 localhost6.localdomain6
192.168.11.5 hirs_aca.ad.ent1.sca.nccoe.nist.gov hirs_aca
```



```
  GNU nano 2.3.1                             File: /etc/hostname                                   Modified

hirs-aca
```



```
  GNU nano 2.3.1                             File: /etc/resolv.conf                                Modified

; generated by /usr/sbin/dhclient-script
search ent1.sca.nccoe.nist.gov
nameserver 192.168.11.2
```

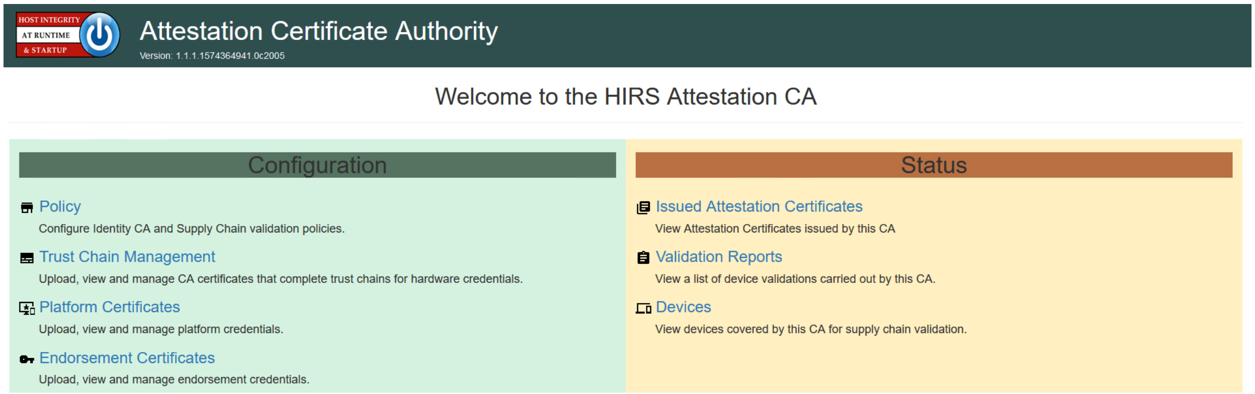
2. Install the HIRS-ACA dependencies using the following command. This will install MySQL/MariaDB, OpenSSL, Tomcat, Java, RPM Dev Tools, GNU Core Utilities, and other Linux commands (initscripts, chkconfig, sed, grep, firewalld, and policycoreutils).

```
# sudo yum install mariadb-server openssl tomcat java-1.8.0 rpmdevtools
coreutils initscripts chkconfig sed grep firewalld policycoreutils
```

3. Download the latest version of HIRS ACA from the Release page on GitHub and execute the following command to install the HIRS ACA.

   ```
   # sudo yum install HIRS_AttestationCA*.rpm
   ```

Ensure the installation was successful by navigating to the dashboard using the FQDN configured above. It should look like the screenshot below.



Attestation Certificate Authority

Version: 1.1.1.1574364941.0c2005

Welcome to the HIRS Attestation CA

Configuration

- Policy
  Configure Identity CA and Supply Chain validation policies.
- Trust Chain Management
  Upload, view and manage CA certificates that complete trust chains for hardware credentials.
- Platform Certificates
  Upload, view and manage platform credentials.
- Endorsement Certificates
  Upload, view and manage endorsement credentials.

Status

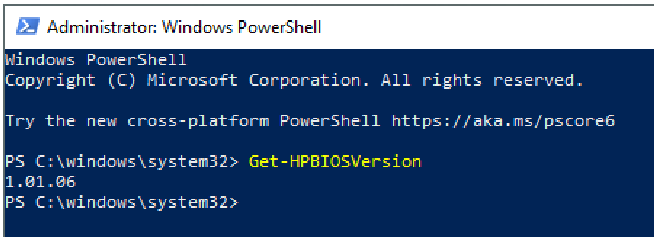
- Issued Attestation Certificates
  View Attestation Certificates issued by this CA
- Validation Reports
  View a list of device validations carried out by this CA.
- Devices
  View devices covered by this CA for supply chain validation.

2.5 HP Inc.

The following steps install the HP Client Management Script Library (CMSL) and execute prerequisite provisioning for HP Inc. laptops. The CMSL installs several PowerShell commands on the laptop that will assist in platform validation. Once CMSL is installed, an administrator configures the HP Inc. specific device security feature. In this prototype demonstration, the target computing device was an HP Inc. Elitebook 360 830 G5.

2.5.1.1 Install the HP CMSL

1. Download the latest CSML from the HP Developers website onto the target HP Inc. laptop.
2. Launch the executable file and proceed through the wizard. Accept the agreement and click **Next**.
3. Select **Install into PowerShell path** and click **Next**.
4. Click **Install**.
5. Click **Finish**.
6. Test the installation by opening PowerShell as an administrator and executing a CMSL command such as `Get-HPBIOSVersion`.



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\windows\system32> Get-HPBIOSVersion
1.01.06
PS C:\windows\system32>
```

2.5.1.2 Execute Provisioning Steps

The next steps are used to provision the HP Inc. specific firmware and device security features, HP Sure Start, HP Sure Admin, HP Tamperlock, and HP Sure Recover. Implementers may also want to consult the HP Inc. Developers Blog for more information on how these payloads were created. Using the example provisioning payloads available from our project repository, use the CMSL to apply the six provisioning payloads as shown below:

1. Open PowerShell as an administrative user. Execute the following commands.

   ```
   Set-HPSecurePlatformPayload -PayloadFile EKProvisionPayload.dat
   Set-HPSecurePlatformPayload -PayloadFile SKProvisionPayload.dat
   ```

2. Reboot the laptop. A local administrator must accept the *Physical Presence Prompt* to complete provisioning of the Endorsement and Signing Key.
3. Execute the following commands from PowerShell as an administrator.

   ```
   Set-HPSecurePlatformPayload -PayloadFile EnableEBAMPayload.dat
   Set-HPSecurePlatformPayload -PayloadFile LAKProvisionPayload.dat
   ```

4. Reboot the laptop. This will expose settings that require a BIOS administrator be configured before the next step can be completed.
5. Execute the following commands from PowerShell as an administrator.

   ```
   Set-HPSecurePlatformPayload -PayloadFile BIOSsettingsPayloadFile.dat
   Set-HPSecurePlatformPayload -PayloadFile SureRecoverProvision.dat
   ```

2.6 Hewlett Packard Enterprise (HPE)

This section will be updated to address HPE servers in a future version of this publication.

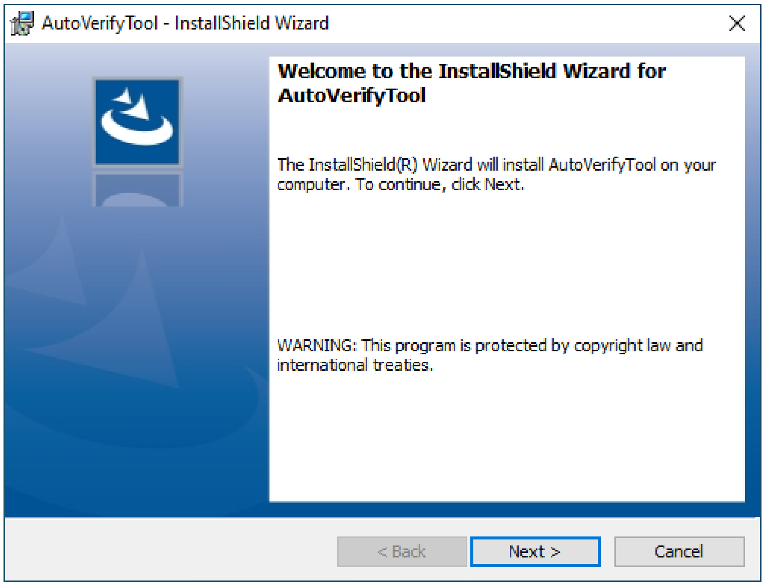
2.7 Intel

The Intel Transparent Supply Chain (TSC) requires two client applications to support acceptance testing and continuous monitoring scenarios: TSCVerifyUtil and AutoVerifyTool. Contact your Intel representative to download the installation packages for both utilities. Once the binaries have been retrieved, follow these procedures on the target laptop. Table 2-3 lists the laptops used within this demonstration.

Table 2-3 Intel-Contributed Laptops

Machine Name	Operating System	Manufacturer	Model
intel-0	Windows 10	HP Inc.	Elitebook 360 830 G5
intel-1	Windows 10	Lenovo	ThinkPad T480

1. Download and install the latest Microsoft Visual C++ Redistributable for Visual Studio.
2. Launch the AutoVerifyTool installation wizard. Click **Next**.



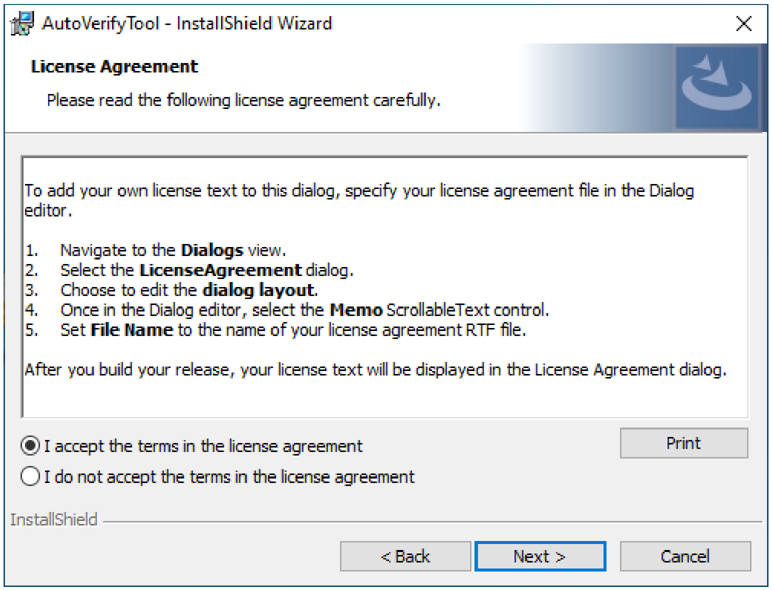
AutoVerifyTool - InstallShield Wizard

Welcome to the InstallShield Wizard for AutoVerifyTool

The InstallShield(R) Wizard will install AutoVerifyTool on your computer. To continue, click Next.

WARNING: This program is protected by copyright law and international treaties.

3. Accept the license and client **Next**.



License Agreement

Please read the following license agreement carefully.

To add your own license text to this dialog, specify your license agreement file in the Dialog editor.

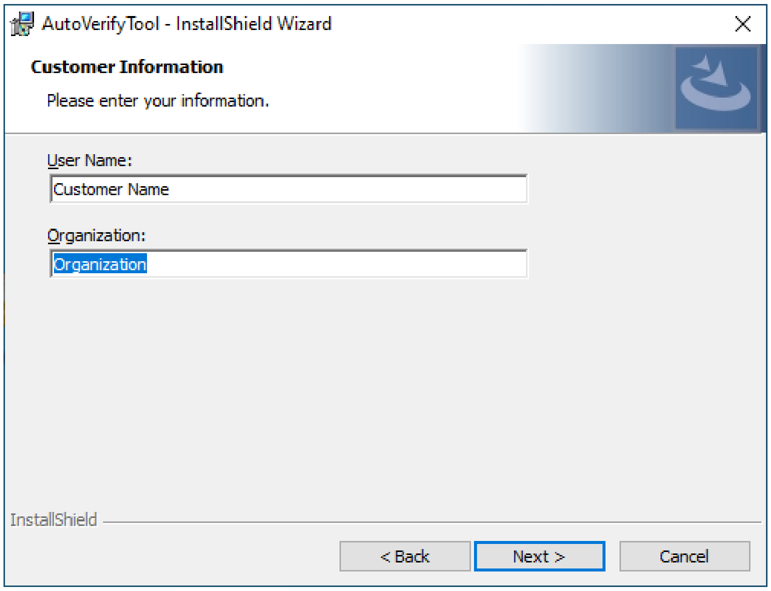
1. Navigate to the **Dialogs** view.
2. Select the **LicenseAgreement** dialog.
3. Choose to edit the **dialog layout**.
4. Once in the Dialog editor, select the **Memo** ScrollableText control.
5. Set **File Name** to the name of your license agreement RTF file.

After you build your release, your license text will be displayed in the License Agreement dialog.

● I accept the terms in the license agreement

○ I do not accept the terms in the license agreement

4. Enter your Name and Organization. Click **Next**.



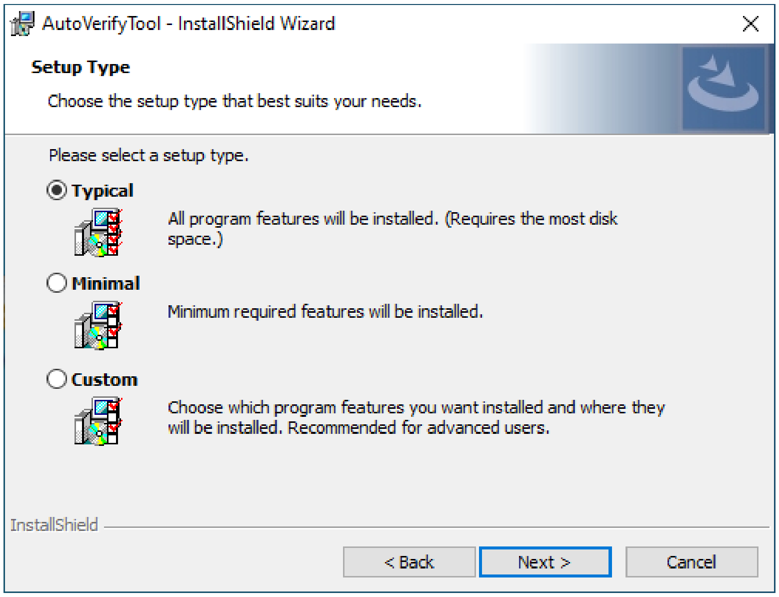
Customer Information

Please enter your information.

User Name: Customer Name

Organization: Organization

5. Select the **Typical** installation. Click **Next**.



AutoVerifyTool - InstallShield Wizard

Setup Type

Choose the setup type that best suits your needs.

Please select a setup type.

● **Typical**

All program features will be installed. (Requires the most disk space.)

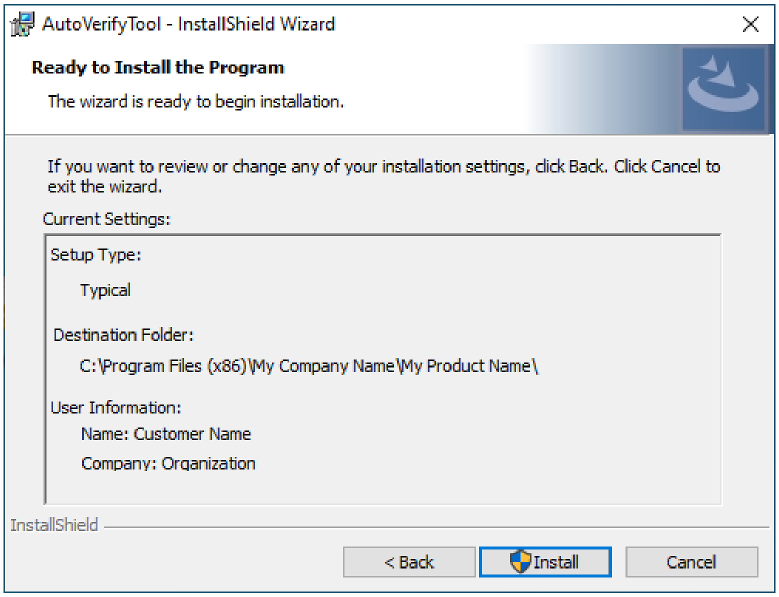
○ **Minimal**

Minimum required features will be installed.

○ **Custom**

Choose which program features you want installed and where they will be installed. Recommended for advanced users.

6. Click **Install**.



AutoVerifyTool - InstallShield Wizard

Ready to Install the Program

The wizard is ready to begin installation.

If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.

Current Settings:

Setup Type:

Typical

Destination Folder:

C:\Program Files (x86)\My Company Name\My Product Name\

User Information:

Name: Customer Name

Company: Organization

2.8 RSA Archer

This section describes the installation of the RSA Archer system for this demonstration. Our instantiation of RSA Archer is viable for a lab environment, but the reader is encouraged to refer to the architecture planning guide on the RSA Archer website for specific guidance for your environment. We elected to install the RSA Archer system across two virtual machines – one hosting a Microsoft SQL database and the other hosting the remainder of the RSA Archer services.

Table 2-4 shows the system information used in this prototype demonstration for RSA Archer.

Table 2-4 RSA Archer System Information

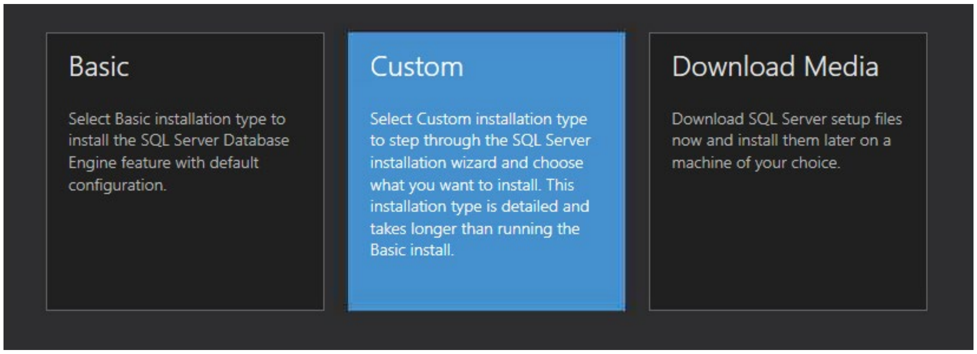
Machine Name	Machine Type	Operating System
Archer Database Server	Virtual	Windows 2019 Server
Archer Services	Virtual	Windows 2019 Server

2.8.1 Prerequisites

Before installing RSA Archer services, several prerequisites must be fulfilled. In this section, we will describe those prerequisites involving the database server and Microsoft's Internet Information Services (IIS) web server.

2.8.1.1 Install SQL Server on Database Server

1. Download SQL Server 2019 from https://www.microsoft.com/en-us/sql-server/sql-server-downloads onto the database server.
2. Run the SQL Server 2019 executable.
3. Select the **Custom** installation type.



Basic

Select Basic installation type to install the SQL Server Database Engine feature with default configuration.

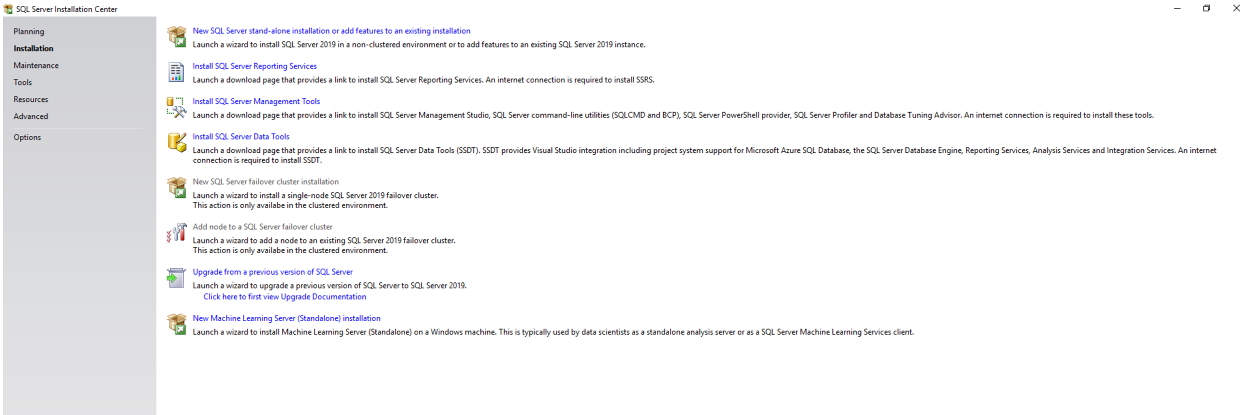
Custom

Select Custom installation type to step through the SQL Server installation wizard and choose what you want to install. This installation type is detailed and takes longer than running the Basic install.

Download Media

Download SQL Server setup files now and install them later on a machine of your choice.

4. Specify the download location and select **Install.**
5. Allow the installer to download the SQL Server 2019 package.
6. The SQL Server Installation Center should automatically open. From the left menu panel, select **Installation.** Select the option **New SQL Server stand-alone installation or add features to an existing installation**.



New SQL Server stand-alone installation or add features to an existing installation
Launch a wizard to install SQL Server 2019 in a non-clustered environment or to add features to an existing SQL Server 2019 instance.

Install SQL Server Reporting Services
Launch a download page that provides a link to install SQL Server Reporting Services. An internet connection is required to install SSRS.

Install SQL Server Management Tools
Launch a download page that provides a link to install SQL Server Management Studio, SQL Server command-line utilities (SQLCMD and BCP), SQL Server PowerShell provider, SQL Server Profiler and Database Tuning Advisor. An internet connection is required to install these tools.

Install SQL Server Data Tools
Launch a download page that provides a link to install SQL Server Data Tools (SSDT). SSDT provides Visual Studio integration including project system support for Microsoft Azure SQL Database, the SQL Server Database Engine, Reporting Services, Analysis Services and Integration Services. An internet connection is required to install SSDT.

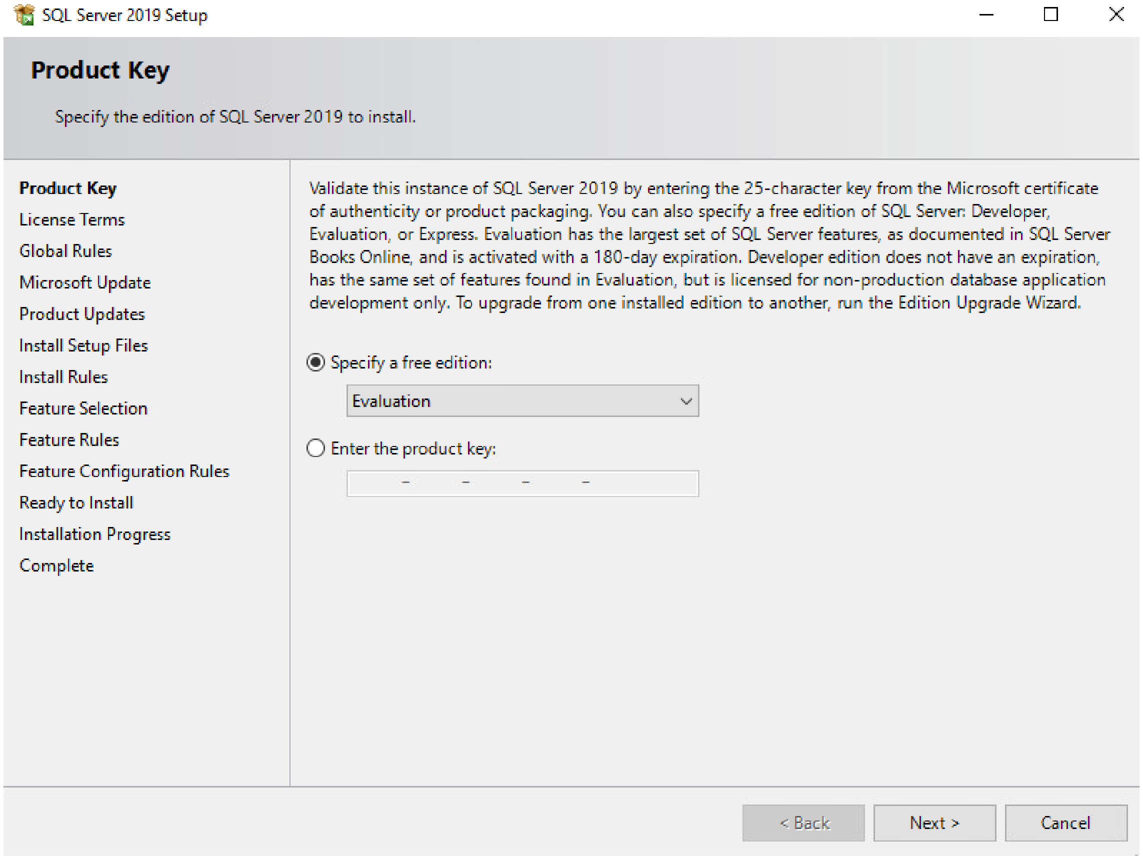
New SQL Server failover cluster installation
Launch a wizard to install a single-node SQL Server 2019 failover cluster.
This action is only availabe in the clustered environment.

Add node to a SQL Server failover cluster
Launch a wizard to add a node to an existing SQL Server 2019 failover cluster.
This action is only availabe in the clustered environment.

Upgrade from a previous version of SQL Server
Launch a wizard to upgrade a previous version of SQL Server to SQL Server 2019.
Click here to first view Upgrade Documentation

New Machine Learning Server (Standalone) installation
Launch a wizard to install Machine Learning Server (Standalone) on a Windows machine. This is typically used by data scientists as a standalone analysis server or as a SQL Server Machine Learning Services client.

7. Enter the product key or select a free edition of the software. Then select **Next.**



Product Key

Specify the edition of SQL Server 2019 to install.

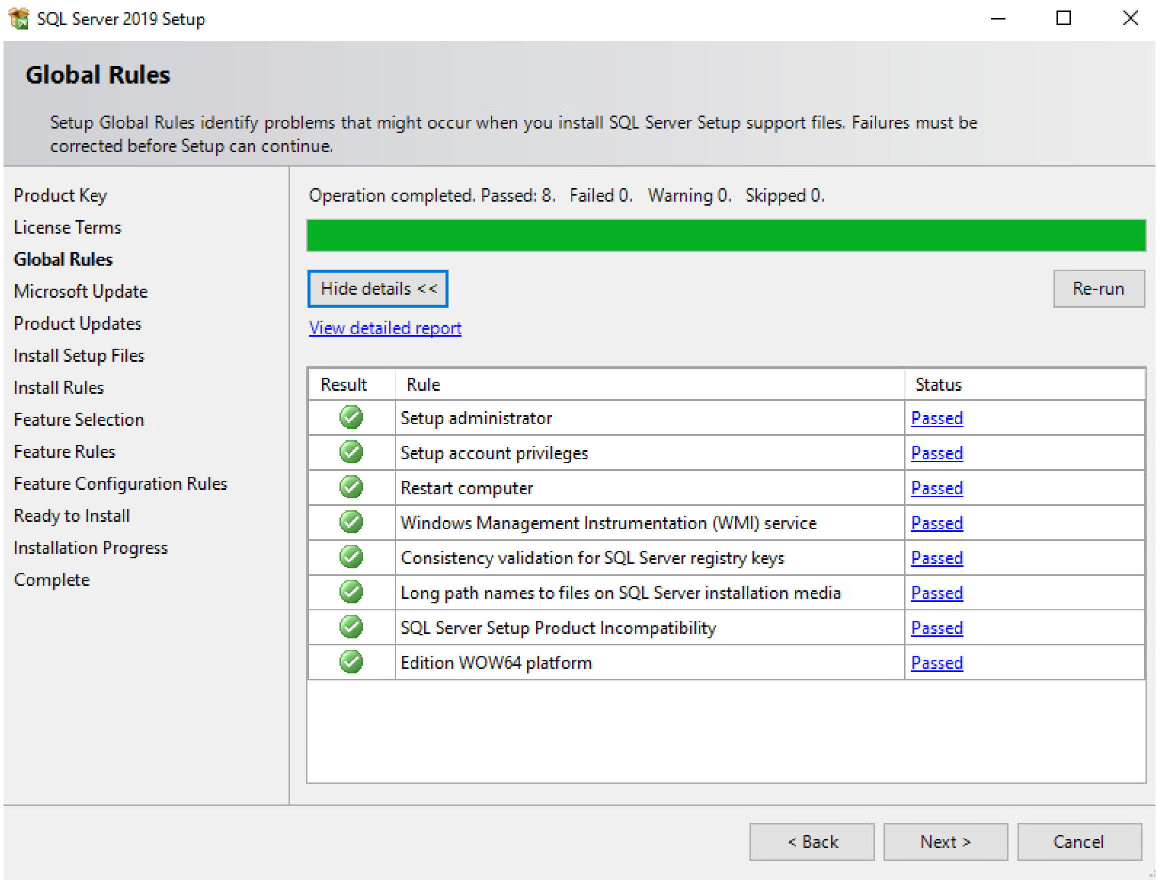
Validate this instance of SQL Server 2019 by entering the 25-character key from the Microsoft certificate of authenticity or product packaging. You can also specify a free edition of SQL Server: Developer, Evaluation, or Express. Evaluation has the largest set of SQL Server features, as documented in SQL Server Books Online, and is activated with a 180-day expiration. Developer edition does not have an expiration, has the same set of features found in Evaluation, but is licensed for non-production database application development only. To upgrade from one installed edition to another, run the Edition Upgrade Wizard.

● Specify a free edition: Evaluation

○ Enter the product key: - - - -

8. Read and accept the License Terms. Then select **Next**.

9. Ensure that all the **Global Rules** have passed. Then select **Next**.



Global Rules

Setup Global Rules identify problems that might occur when you install SQL Server Setup support files. Failures must be corrected before Setup can continue.

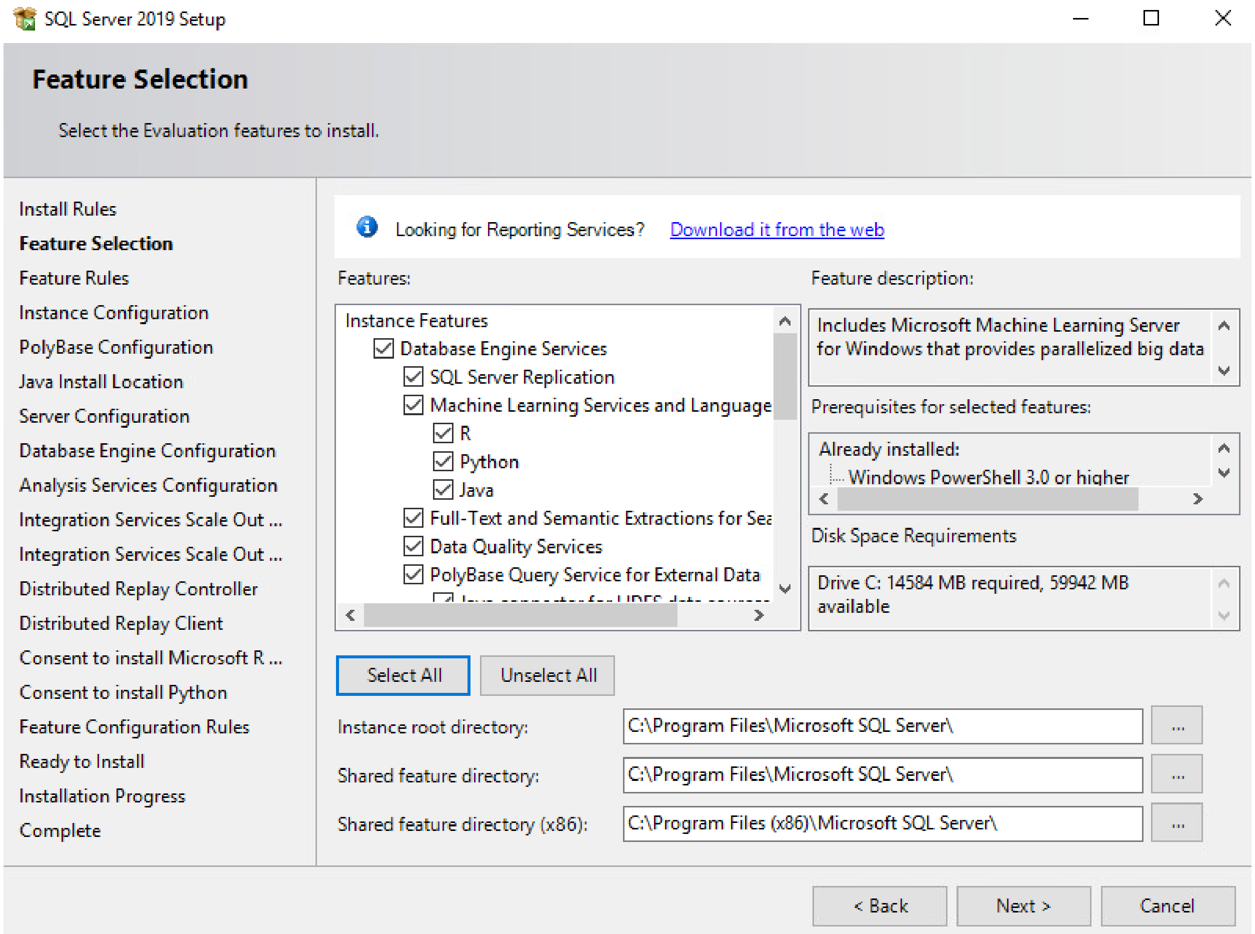
Operation completed. Passed: 8. Failed 0. Warning 0. Skipped 0.

Result	Rule	Status
✓	Setup administrator	Passed
✓	Setup account privileges	Passed
✓	Restart computer	Passed
✓	Windows Management Instrumentation (WMI) service	Passed
✓	Consistency validation for SQL Server registry keys	Passed
✓	Long path names to files on SQL Server installation media	Passed
✓	SQL Server Setup Product Incompatibility	Passed
✓	Edition WOW64 platform	Passed

10. To use Microsoft Update to automatically deliver updates, check the box **Use Microsoft Update to check for updates (recommended).** Then select **Next.**

11. Ensure that all the **Install Rules** have passed. Then select **Next.**

12. Select the desired features to install. Then select **Next.** Complete the sections for the selected features.


SQL Server 2019 Setup
Install Rules
Feature Selection
Feature Rules
Instance Configuration
PolyBase Configuration
Java Install Location
Server Configuration
Database Engine Configuration
Analysis Services Configuration
Integration Services Scale Out ...
Integration Services Scale Out ...
Distributed Replay Controller
Distributed Replay Client
Consent to install Microsoft R ...
Consent to install Python
Feature Configuration Rules
Ready to Install
Installation Progress
Complete
Select All
Unselect All
...
< Back
Next >
Cancel

Feature Selection

Select the Evaluation features to install.

Looking for Reporting Services? Download it from the web

Features:

Instance Features
- ☑ Database Engine Services
  - ☑ SQL Server Replication
  - ☑ Machine Learning Services and Language
    - ☑ R
    - ☑ Python
    - ☑ Java
  - ☑ Full-Text and Semantic Extractions for Sea
  - ☑ Data Quality Services
  - ☑ PolyBase Query Service for External Data
    - ☑ Java connector for HDFS data sources

Feature description:

Includes Microsoft Machine Learning Server for Windows that provides parallelized big data

Prerequisites for selected features:

Already installed:
Windows PowerShell 3.0 or higher

Disk Space Requirements

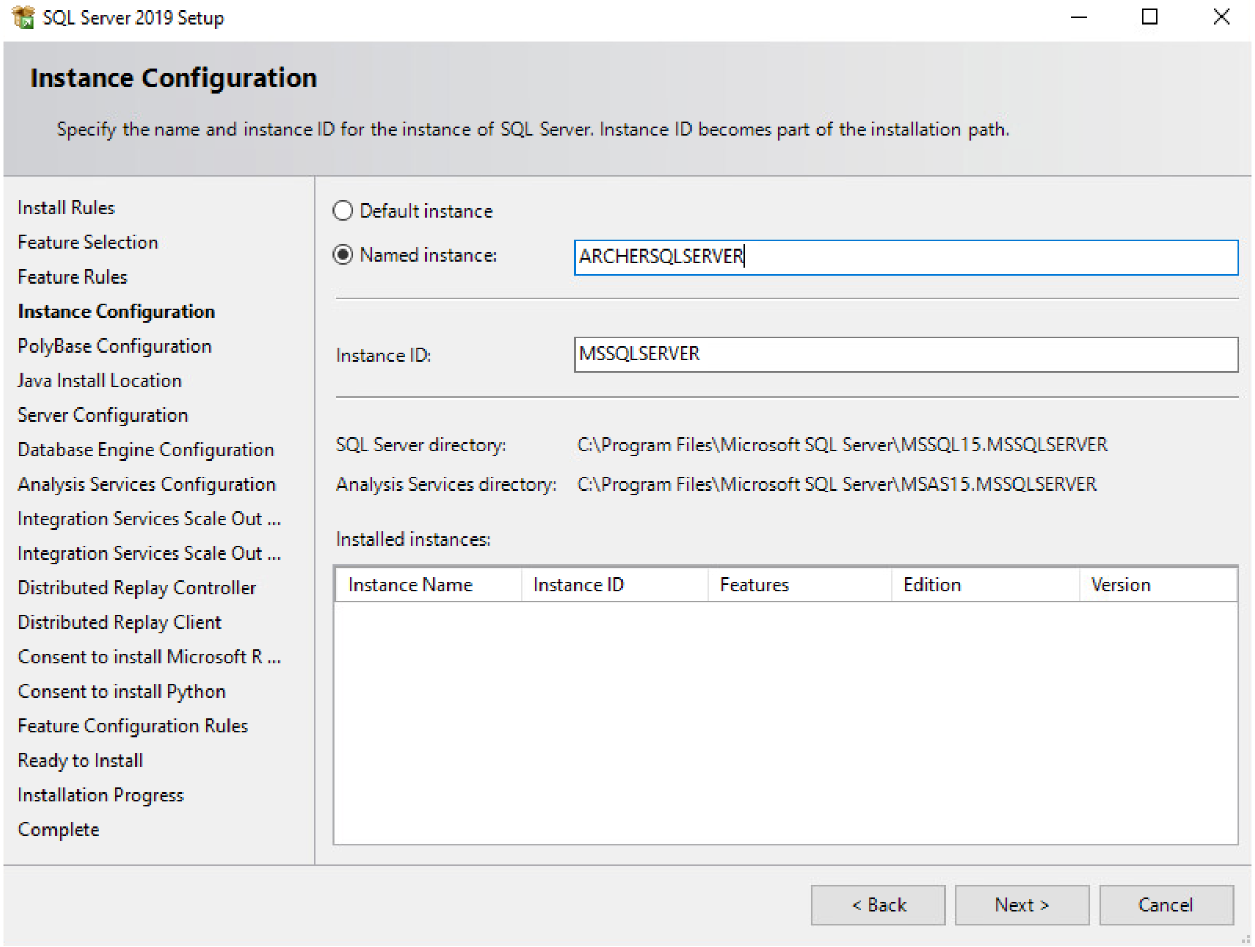
Drive C: 14584 MB required, 59942 MB available

Instance root directory: C:\Program Files\Microsoft SQL Server\

Shared feature directory: C:\Program Files\Microsoft SQL Server\

Shared feature directory (x86): C:\Program Files (x86)\Microsoft SQL Server\

13. In the **Instance Configuration** section, select the **Named instance** radio button and choose a name for the database server, or select the **Default instance** radio button to use the default name. Then select **Next.**



SQL Server 2019 Setup

Instance Configuration

Specify the name and instance ID for the instance of SQL Server. Instance ID becomes part of the installation path.

Install Rules
Feature Selection
Feature Rules
Instance Configuration
PolyBase Configuration
Java Install Location
Server Configuration
Database Engine Configuration
Analysis Services Configuration
Integration Services Scale Out ...
Integration Services Scale Out ...
Distributed Replay Controller
Distributed Replay Client
Consent to install Microsoft R ...
Consent to install Python
Feature Configuration Rules
Ready to Install
Installation Progress
Complete

○ Default instance

● Named instance: ARCHERSQLSERVER

Instance ID: MSSQLSERVER

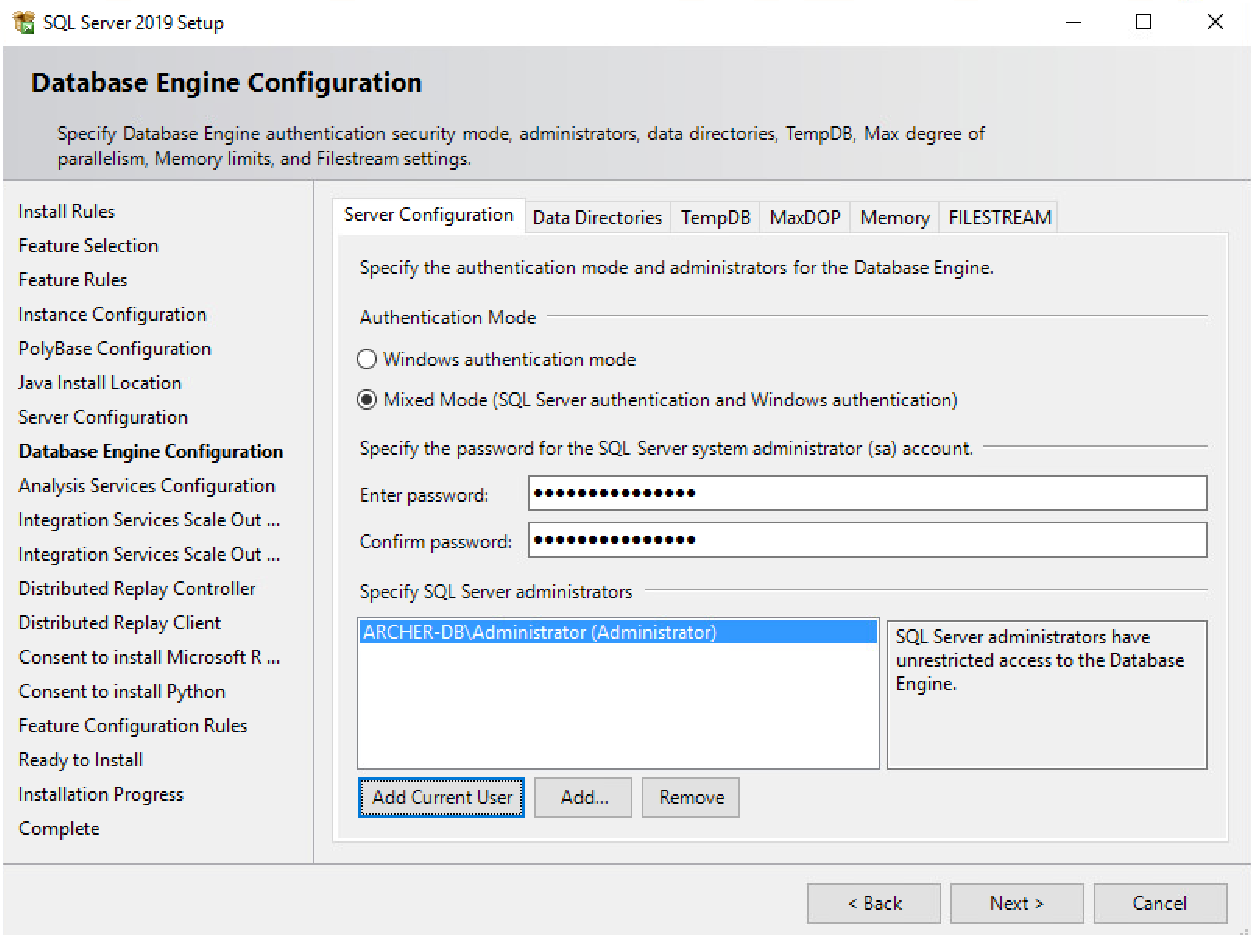
SQL Server directory: C:\Program Files\Microsoft SQL Server\MSSQL15.MSSQLSERVER

Analysis Services directory: C:\Program Files\Microsoft SQL Server\MSAS15.MSSQLSERVER

Installed instances:

Instance Name	Instance ID	Features	Edition	Version

14. In the **Database Engine Configuration** section, select the desired Authentication Mode. Select **Add Current User** to add the current user as a SQL Server administrator and select **Next.**



SQL Server 2019 Setup

Database Engine Configuration

Specify Database Engine authentication security mode, administrators, data directories, TempDB, Max degree of parallelism, Memory limits, and Filestream settings.

Specify the authentication mode and administrators for the Database Engine.

Authentication Mode

○ Windows authentication mode

● Mixed Mode (SQL Server authentication and Windows authentication)

Specify the password for the SQL Server system administrator (sa) account.

Enter password: •••••••••••••••

Confirm password: •••••••••••••••

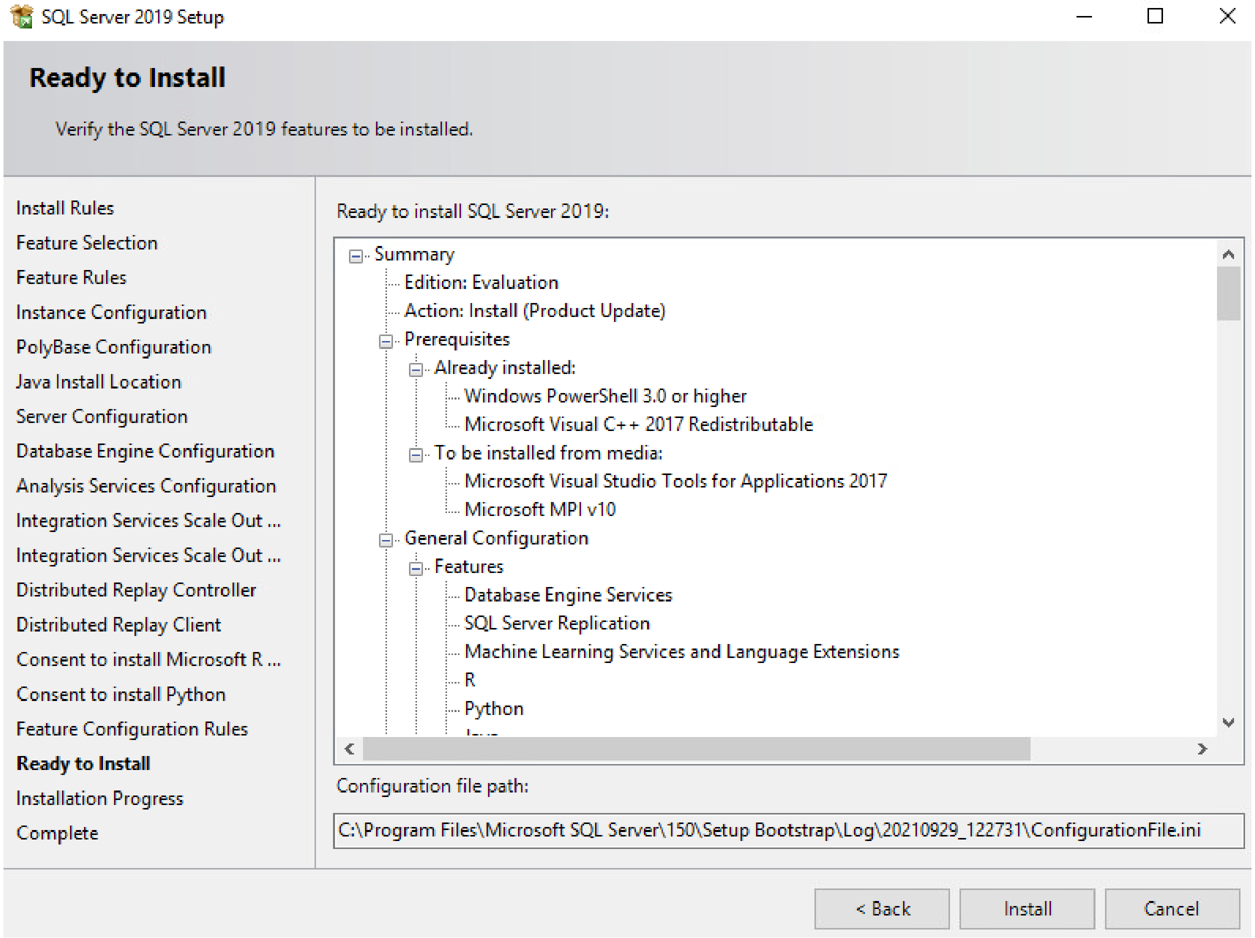
Specify SQL Server administrators

ARCHER-DB\Administrator (Administrator)

SQL Server administrators have unrestricted access to the Database Engine.

15. Ensure that all the **Feature Configuration Rules** have passed and select **Next.**

16. Confirm the selected settings are desired and select **Install.**


SQL Server 2019 Setup
Install Rules
Feature Selection
Feature Rules
Instance Configuration
PolyBase Configuration
Java Install Location
Server Configuration
Database Engine Configuration
Analysis Services Configuration
Integration Services Scale Out ...
Integration Services Scale Out ...
Distributed Replay Controller
Distributed Replay Client
Consent to install Microsoft R ...
Consent to install Python
Feature Configuration Rules
Ready to Install
Installation Progress
Complete
< Back
Install
Cancel

Ready to Install

Verify the SQL Server 2019 features to be installed.

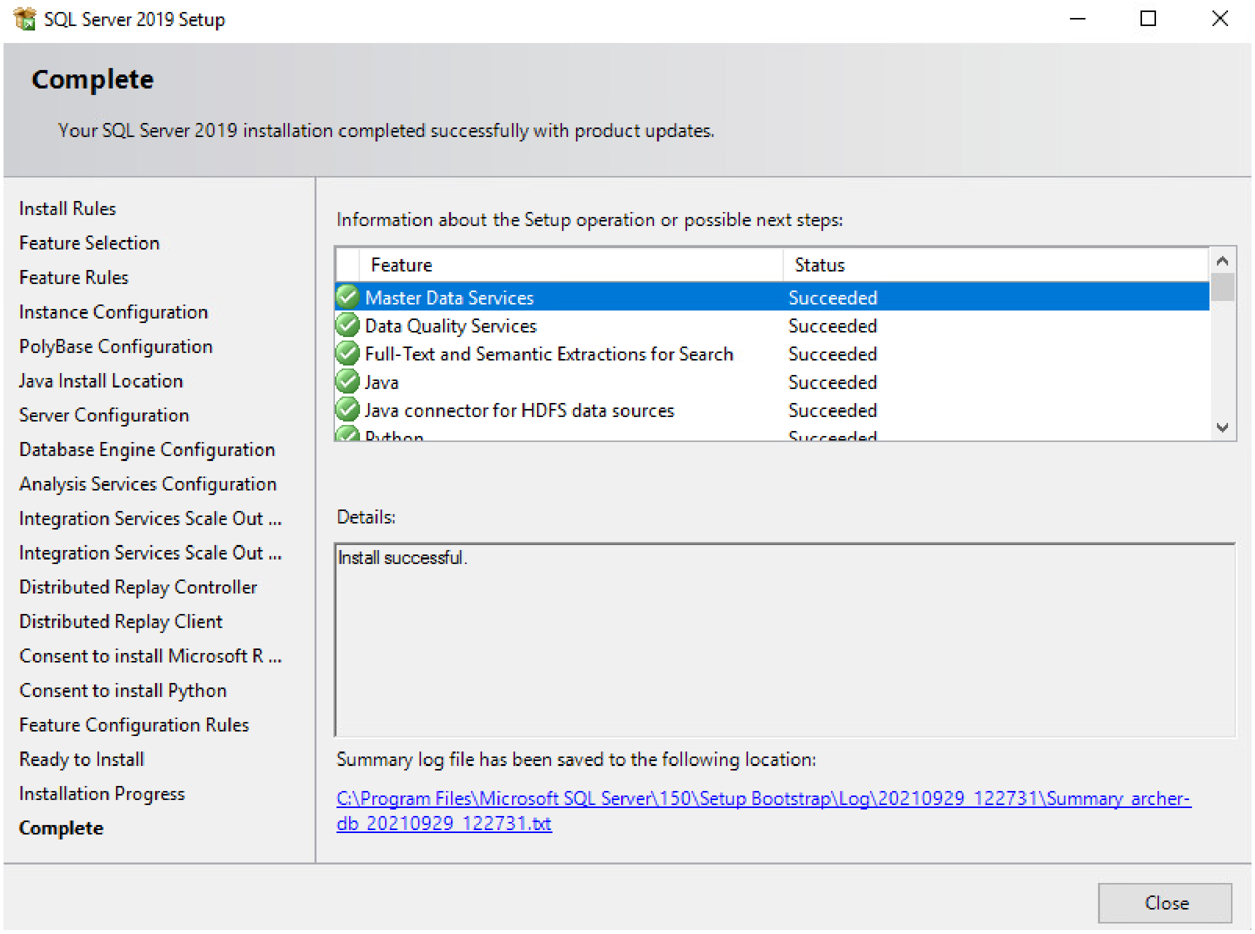
Ready to install SQL Server 2019:

```
Summary
  Edition: Evaluation
  Action: Install (Product Update)
  Prerequisites
    Already installed:
      Windows PowerShell 3.0 or higher
      Microsoft Visual C++ 2017 Redistributable
    To be installed from media:
      Microsoft Visual Studio Tools for Applications 2017
      Microsoft MPI v10
  General Configuration
    Features
      Database Engine Services
      SQL Server Replication
      Machine Learning Services and Language Extensions
      R
      Python
```

Configuration file path:

C:\Program Files\Microsoft SQL Server\150\Setup Bootstrap\Log\20210929_122731\ConfigurationFile.ini

17. Once the installation completes, select **Close.**



SQL Server 2019 Setup
Install Rules
Feature Selection
Feature Rules
Instance Configuration
PolyBase Configuration
Java Install Location
Server Configuration
Database Engine Configuration
Analysis Services Configuration
Integration Services Scale Out ...
Integration Services Scale Out ...
Distributed Replay Controller
Distributed Replay Client
Consent to install Microsoft R ...
Consent to install Python
Feature Configuration Rules
Ready to Install
Installation Progress
Complete
Close

Complete

Your SQL Server 2019 installation completed successfully with product updates.

Information about the Setup operation or possible next steps:

Feature	Status
✓ Master Data Services	Succeeded
✓ Data Quality Services	Succeeded
✓ Full-Text and Semantic Extractions for Search	Succeeded
✓ Java	Succeeded
✓ Java connector for HDFS data sources	Succeeded
✓ Python	Succeeded

Details:

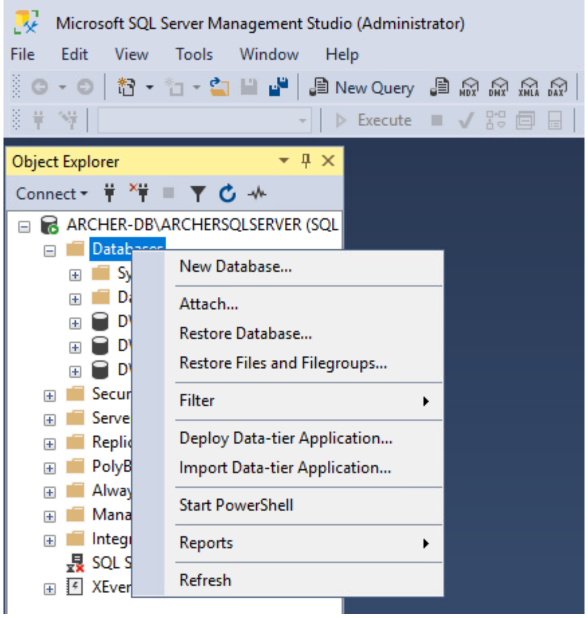
Install successful.

Summary log file has been saved to the following location:

C:\Program Files\Microsoft SQL Server\150\Setup Bootstrap\Log\20210929_122731\Summary_archer-db_20210929_122731.txt

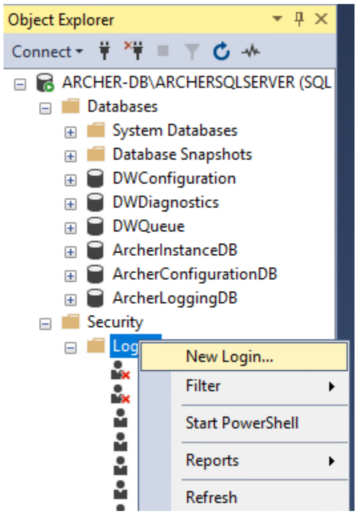
2.8.1.2 Create the RSA Archer Databases

1. Download SQL Server Management Studio (SSMS) from https://aka.ms/ssmsfullsetup. Follow the installation steps.
2. Once installed, open SSMS.
3. Expand the ARCHERSQLSERVER tree. Right-click on **Databases** and select **New Database.** Create three databases: *ArcherInstanceDB*, *ArcherConfigurationDB*, and *ArcherLoggingDB*.


Microsoft SQL Server Management Studio (Administrator)
File
Edit
View
Tools
Window
Help
New Query
Execute
Object Explorer
Connect
ARCHER-DB\ARCHERSQLSERVER (SQL
Databases
New Database...
Attach...
Restore Database...
Restore Files and Filegroups...
Filter
Deploy Data-tier Application...
Import Data-tier Application...
Start PowerShell
Reports
Refresh

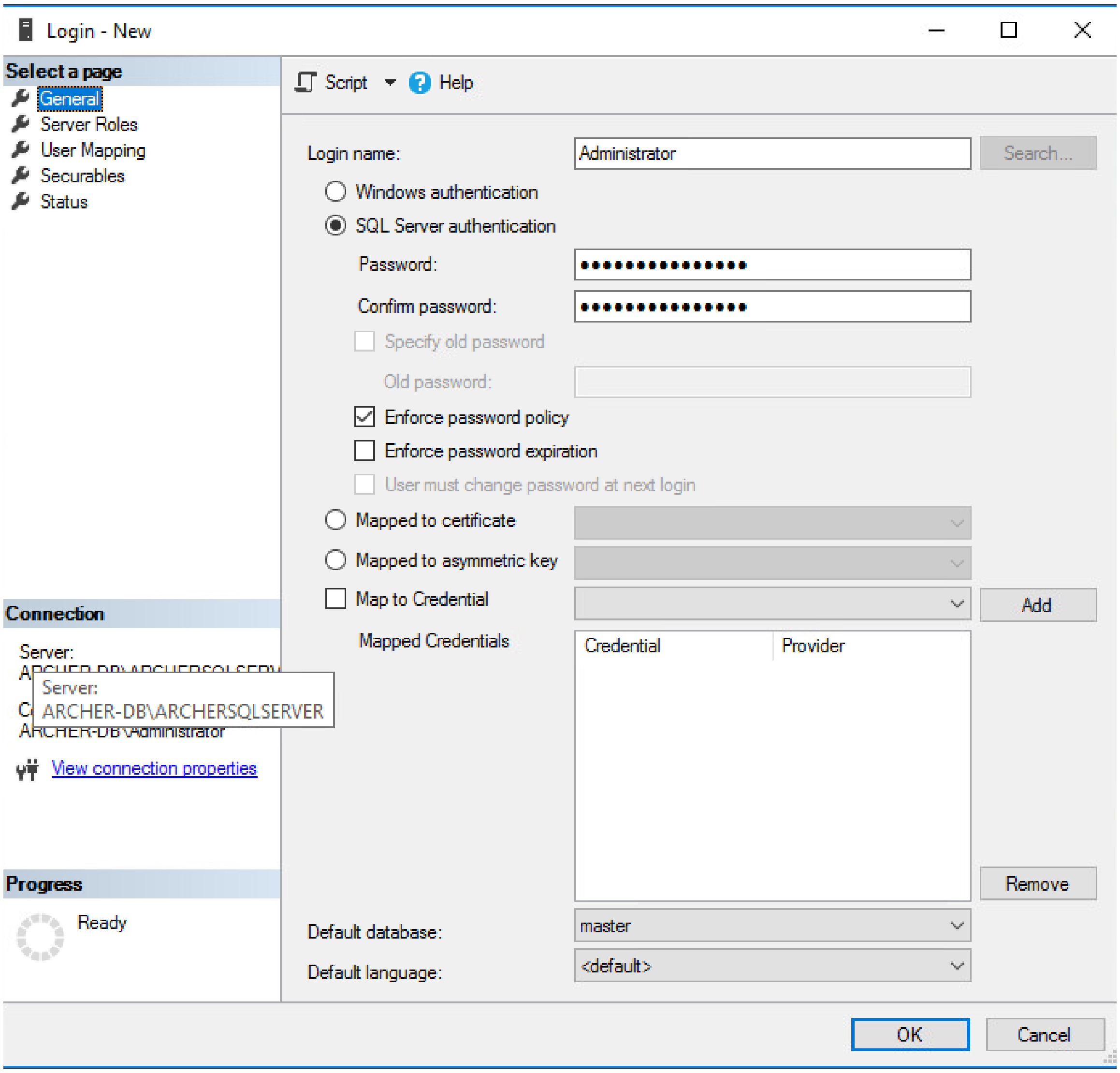
593

594 4. Next, create a local Administrator user. Right-click **Security** and select **New Login.**



595

596 5. Under the **General** tab, input the **Login Name** and select the **SQL Server Authentication** radio
597 button. Create a password for this user. These credentials will be used during the RSA Archer
598 installation.



Login - New

Login name: Administrator

○ Windows authentication

● SQL Server authentication

Password: •••••••••••••••

Confirm password: •••••••••••••••

□ Specify old password

Old password:

☑ Enforce password policy

□ Enforce password expiration

□ User must change password at next login

○ Mapped to certificate

○ Mapped to asymmetric key

□ Map to Credential

Mapped Credentials

Credential	Provider

Default database: master

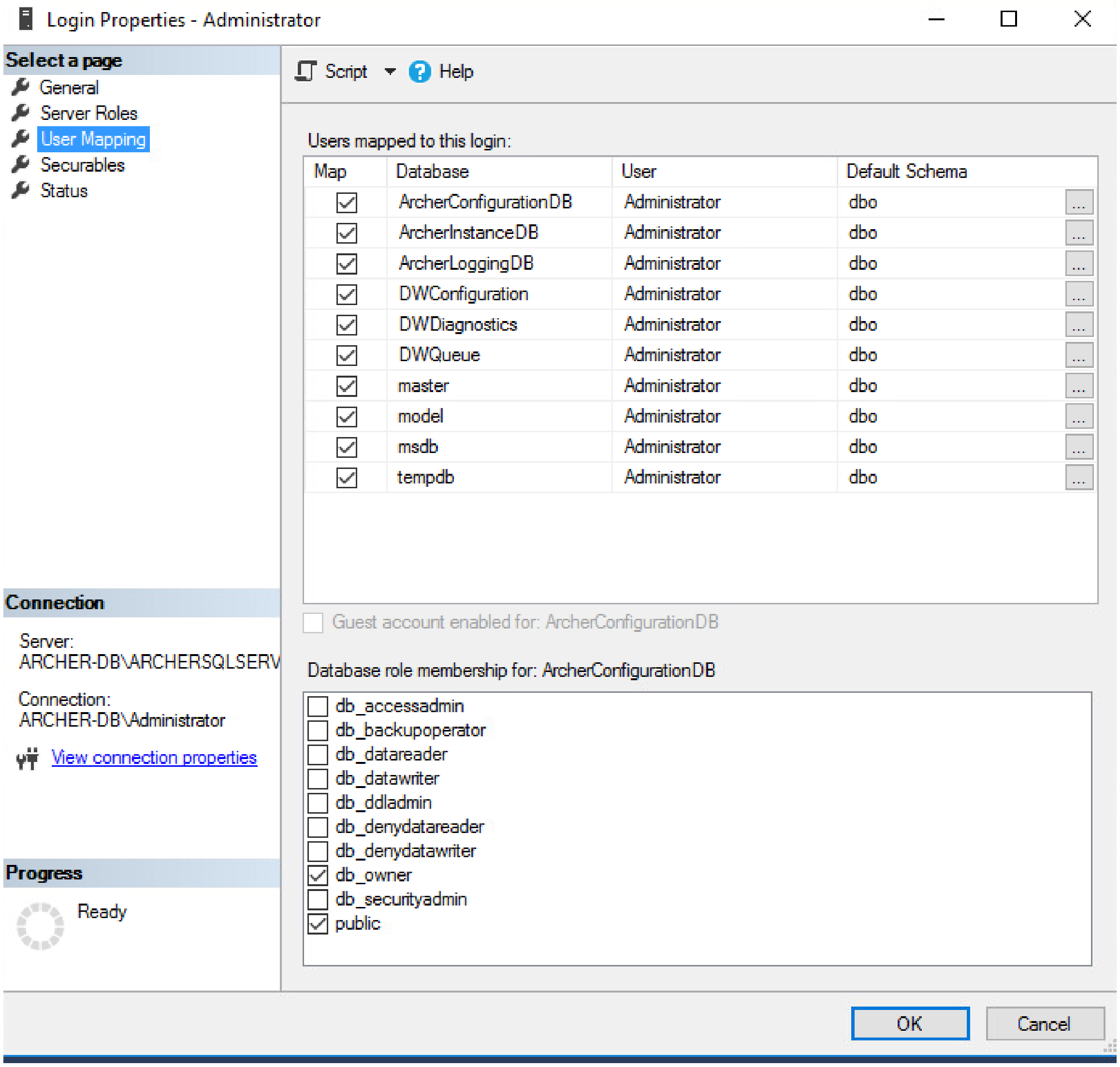
Default language: <default>

Connection

Server:
ARCHER-DB\ARCHERSQLSERVER

Connection:
ARCHER-DB\Administrator

6. Navigate to the **User Mapping** tab. Ensure all the databases have the **Default Schema** set to **dbo**. Also, ensure that **db_owner** is selected for each database under the **Database role membership** section. Select **OK.**



Login Properties - Administrator

Users mapped to this login:

Map	Database	User	Default Schema
☑	ArcherConfigurationDB	Administrator	dbo
☑	ArcherInstanceDB	Administrator	dbo
☑	ArcherLoggingDB	Administrator	dbo
☑	DWConfiguration	Administrator	dbo
☑	DWDiagnostics	Administrator	dbo
☑	DWQueue	Administrator	dbo
☑	master	Administrator	dbo
☑	model	Administrator	dbo
☑	msdb	Administrator	dbo
☑	tempdb	Administrator	dbo

□ Guest account enabled for: ArcherConfigurationDB

Database role membership for: ArcherConfigurationDB

- □ db_accessadmin
- □ db_backupoperator
- □ db_datareader
- □ db_datawriter
- □ db_ddladmin
- □ db_denydatareader
- □ db_denydatawriter
- ☑ db_owner
- □ db_securityadmin
- ☑ public

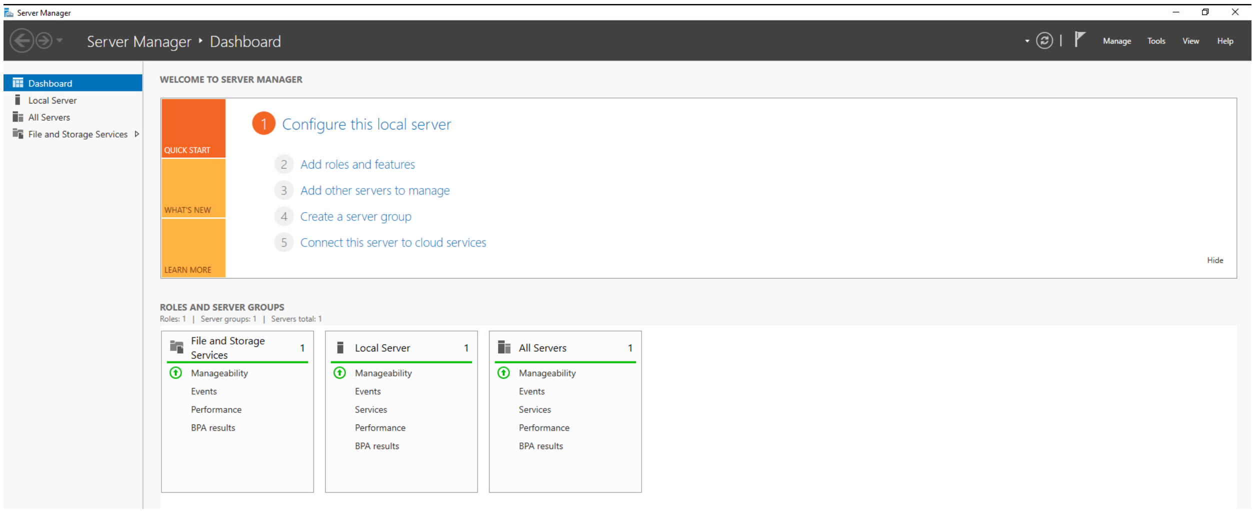
Connection

Server:
ARCHER-DB\ARCHERSQLSERV

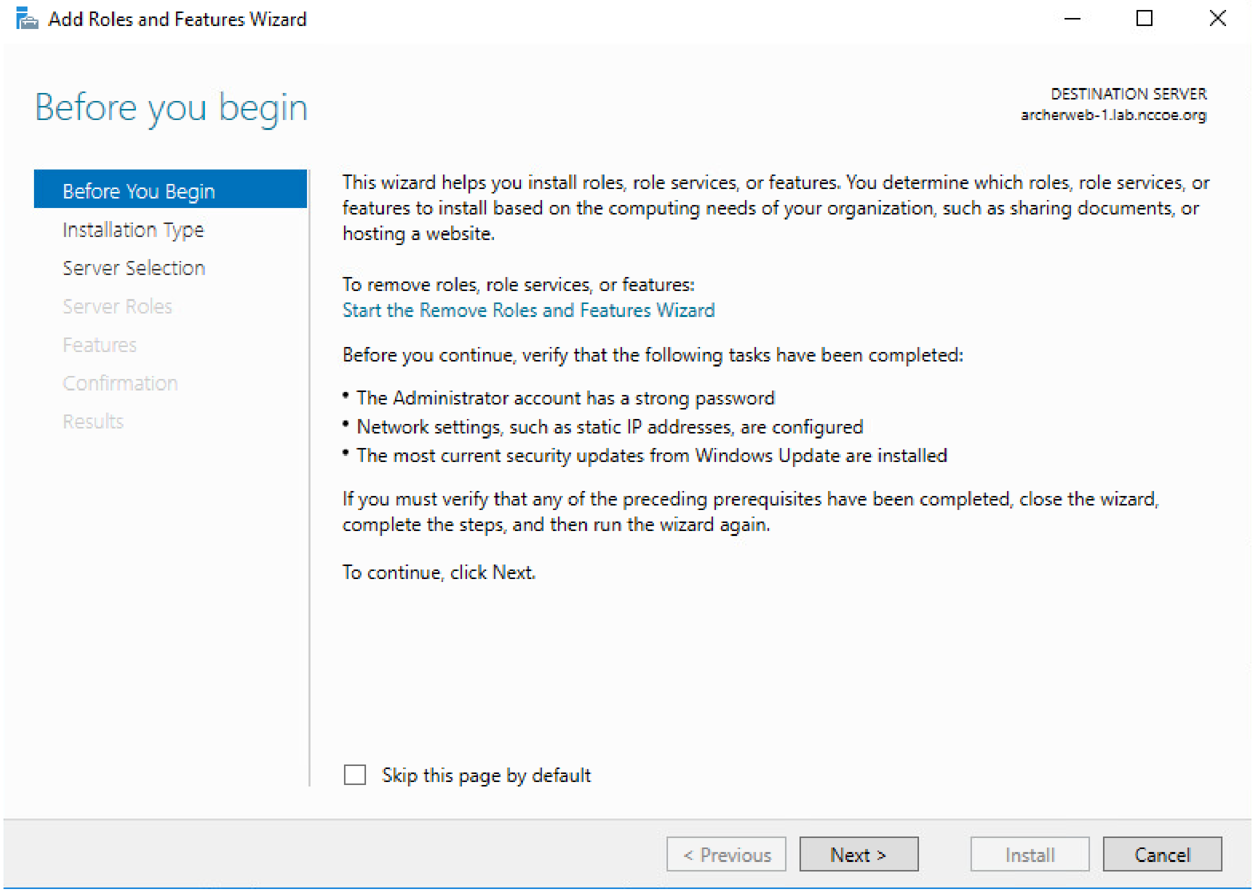
Connection:
ARCHER-DB\Administrator

2.8.1.3 Install Internet Information Services on the Web Server

1. On the web server, open **Server Manager.**



2. Under **Manage**, select **Add Roles and Features**.
3. Select **Next.**



This wizard helps you install roles, role services, or features. You determine which roles, role services, or features to install based on the computing needs of your organization, such as sharing documents, or hosting a website.

To remove roles, role services, or features:
Start the Remove Roles and Features Wizard

Before you continue, verify that the following tasks have been completed:

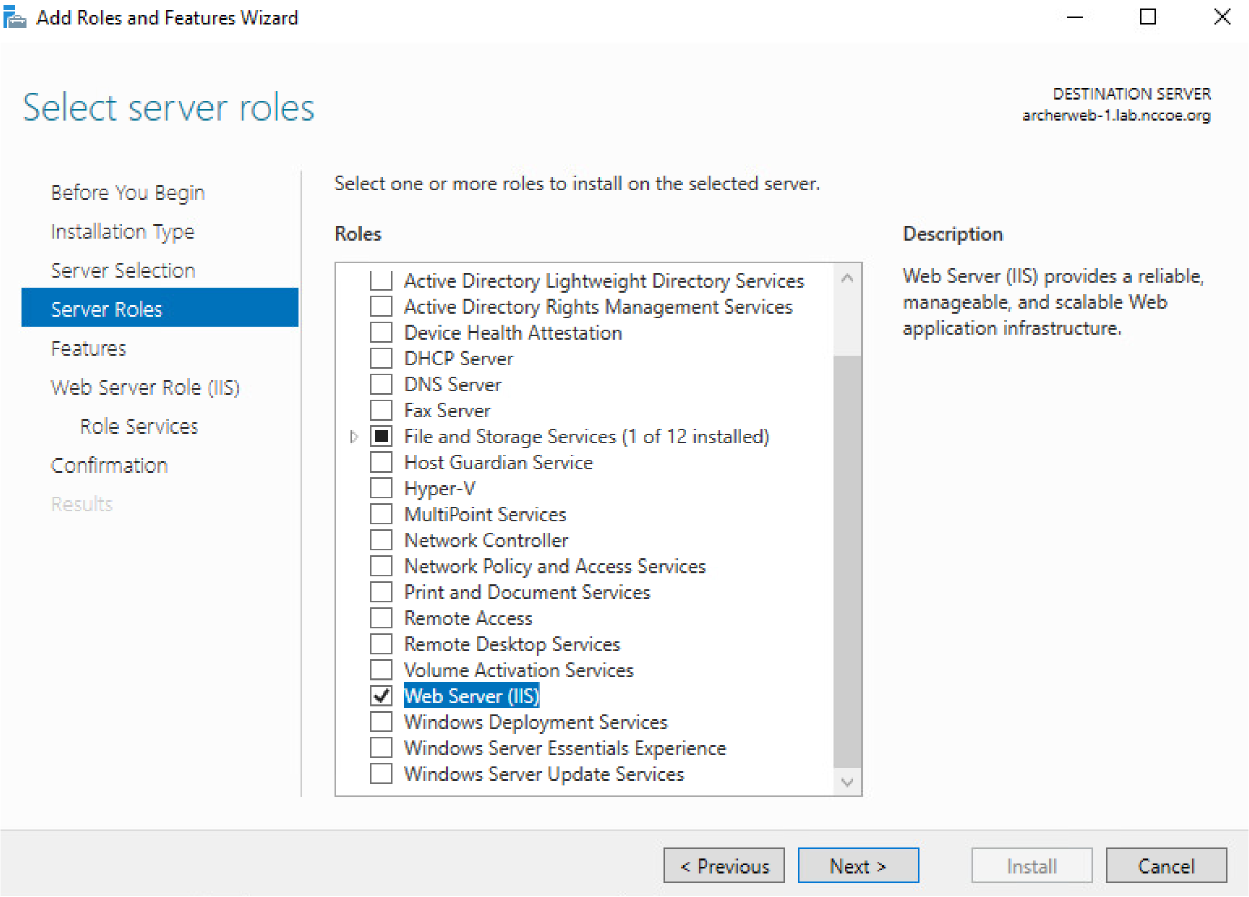
- The Administrator account has a strong password
- Network settings, such as static IP addresses, are configured
- The most current security updates from Windows Update are installed

If you must verify that any of the preceding prerequisites have been completed, close the wizard, complete the steps, and then run the wizard again.

To continue, click Next.

□ Skip this page by default

4. Select the **Role-based or feature-based installation** radio button. Select **Next.**
5. Select the **Web Server (IIS)** server role. Then select **Next.**



Add Roles and Features Wizard

Select server roles

DESTINATION SERVER
archerweb-1.lab.nccoe.org

Select one or more roles to install on the selected server.

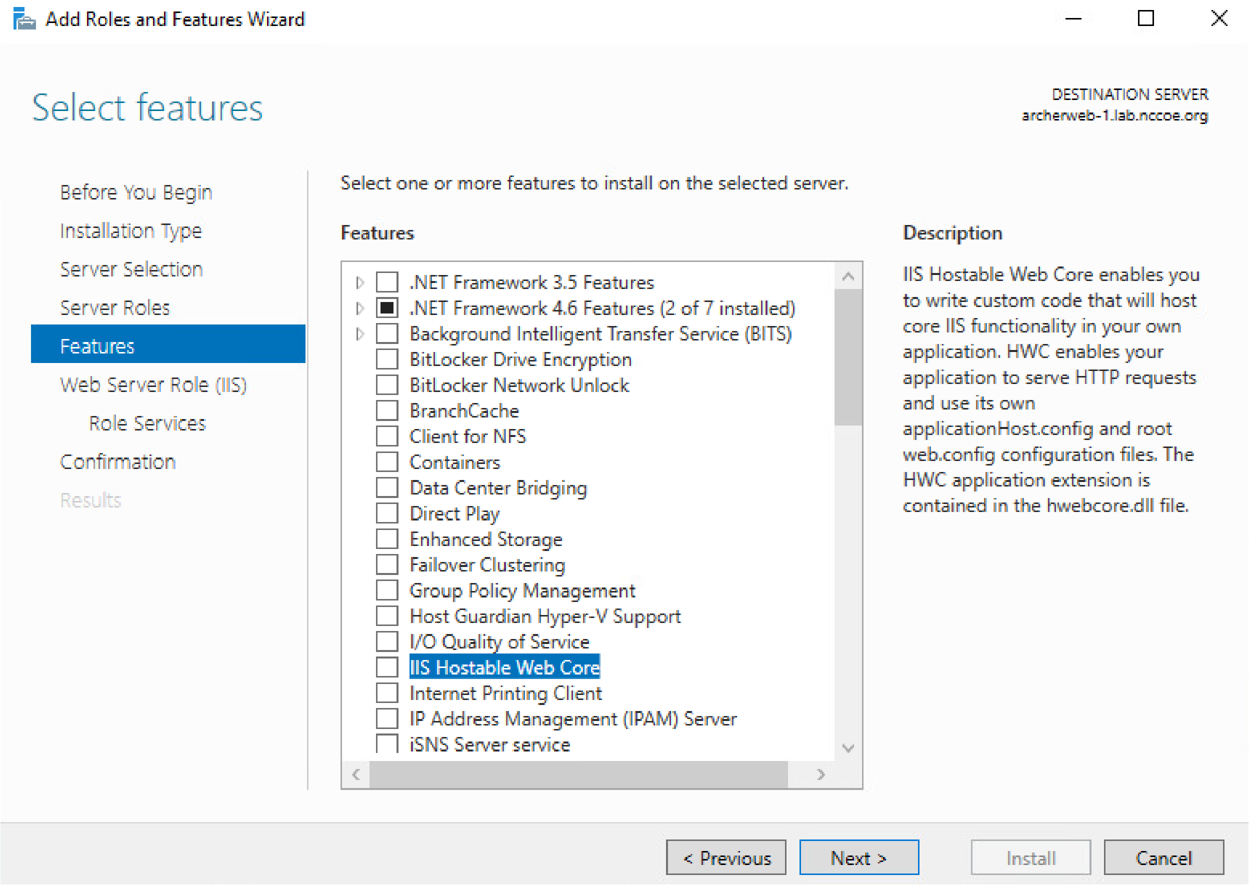
Roles

- □ Active Directory Lightweight Directory Services
- □ Active Directory Rights Management Services
- □ Device Health Attestation
- □ DHCP Server
- □ DNS Server
- □ Fax Server
- ■ File and Storage Services (1 of 12 installed)
- □ Host Guardian Service
- □ Hyper-V
- □ MultiPoint Services
- □ Network Controller
- □ Network Policy and Access Services
- □ Print and Document Services
- □ Remote Access
- □ Remote Desktop Services
- □ Volume Activation Services
- ☑ Web Server (IIS)
- □ Windows Deployment Services
- □ Windows Server Essentials Experience
- □ Windows Server Update Services

Description

Web Server (IIS) provides a reliable, manageable, and scalable Web application infrastructure.

6. In the pop-up window, select **Add Features.**
7. Select **Next.**



Select features

DESTINATION SERVER
archerweb-1.lab.nccoe.org

Select one or more features to install on the selected server.

Features

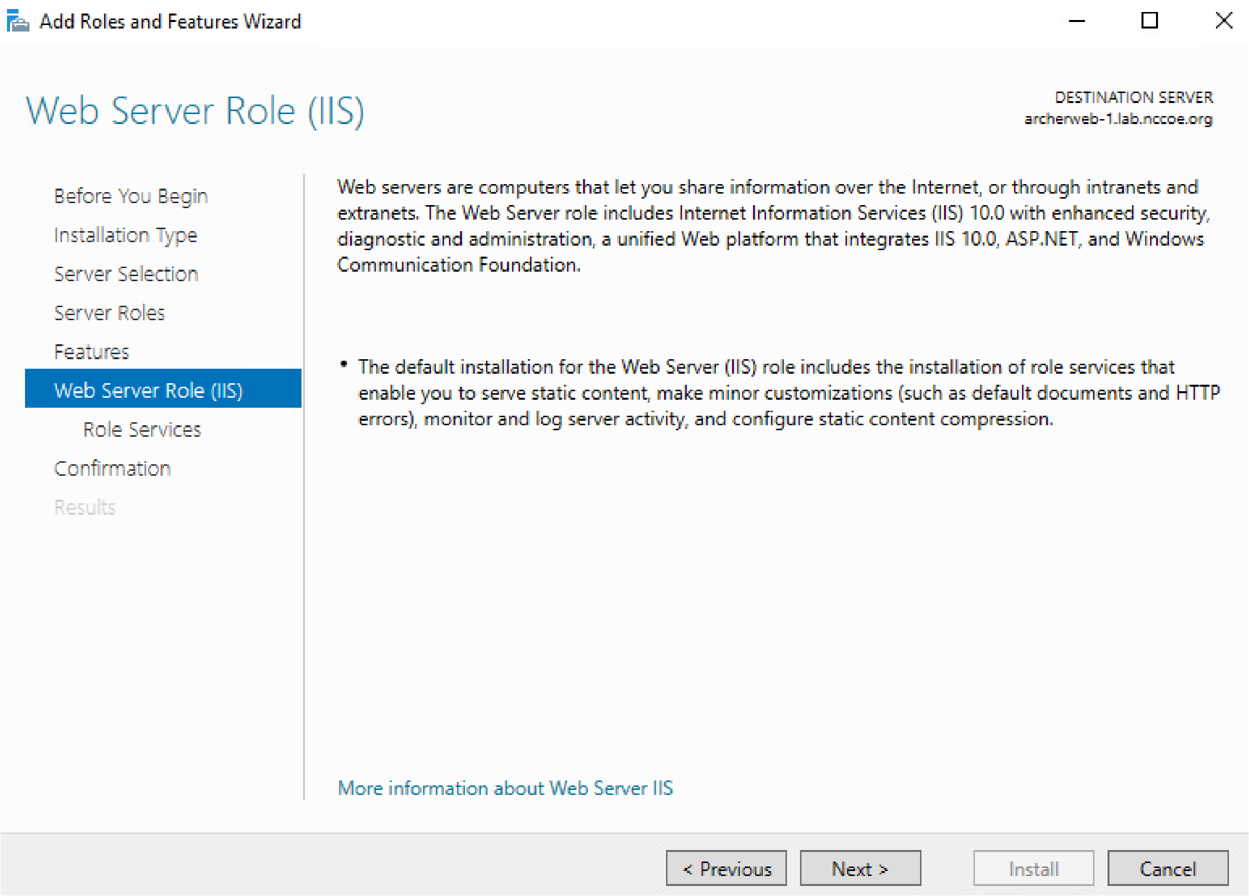
- □ .NET Framework 3.5 Features
- ■ .NET Framework 4.6 Features (2 of 7 installed)
- □ Background Intelligent Transfer Service (BITS)
- □ BitLocker Drive Encryption
- □ BitLocker Network Unlock
- □ BranchCache
- □ Client for NFS
- □ Containers
- □ Data Center Bridging
- □ Direct Play
- □ Enhanced Storage
- □ Failover Clustering
- □ Group Policy Management
- □ Host Guardian Hyper-V Support
- □ I/O Quality of Service
- □ IIS Hostable Web Core
- □ Internet Printing Client
- □ IP Address Management (IPAM) Server
- □ iSNS Server service

Description

IIS Hostable Web Core enables you to write custom code that will host core IIS functionality in your own application. HWC enables your application to serve HTTP requests and use its own applicationHost.config and root web.config configuration files. The HWC application extension is contained in the hwebcore.dll file.

615

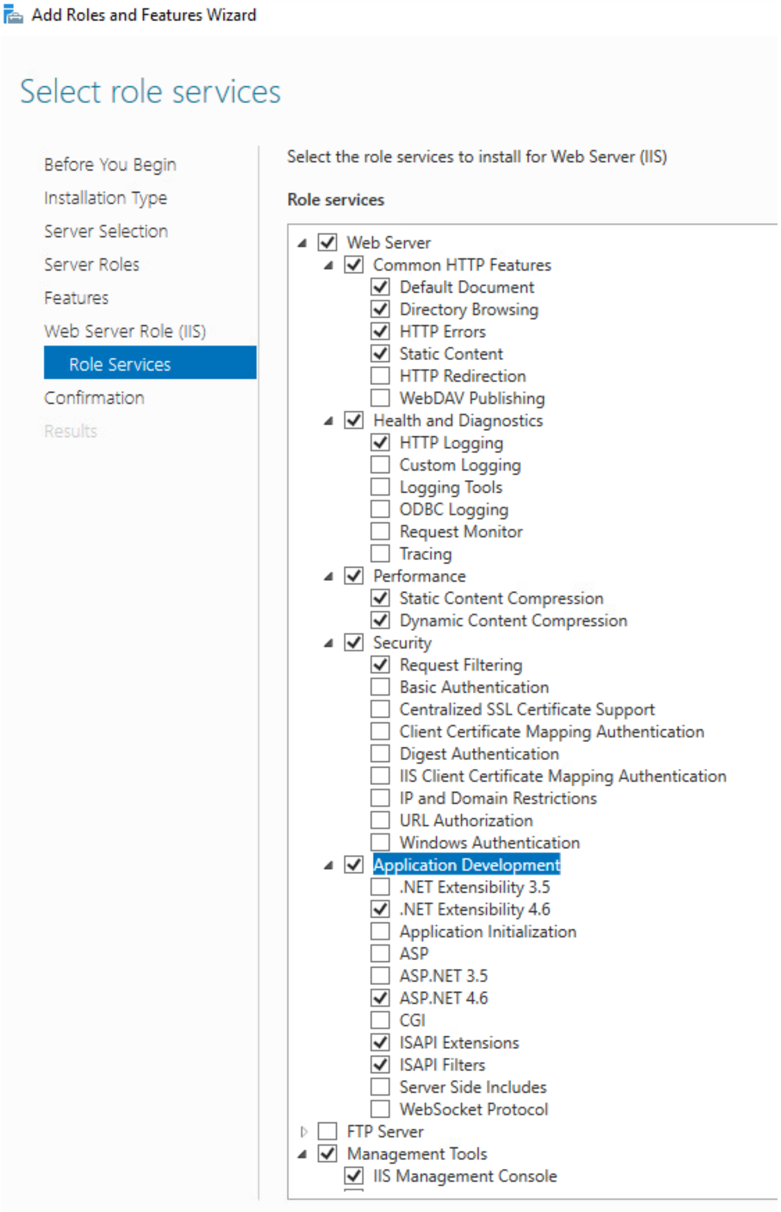
616 8. Select **Next.**



Web servers are computers that let you share information over the Internet, or through intranets and extranets. The Web Server role includes Internet Information Services (IIS) 10.0 with enhanced security, diagnostic and administration, a unified Web platform that integrates IIS 10.0, ASP.NET, and Windows Communication Foundation.

- The default installation for the Web Server (IIS) role includes the installation of role services that enable you to serve static content, make minor customizations (such as default documents and HTTP errors), monitor and log server activity, and configure static content compression.

9. Ensure that the **Role Services** shown below are selected. Then select **Next**.



Add Roles and Features Wizard

Select role services

Select the role services to install for Web Server (IIS)

Role services

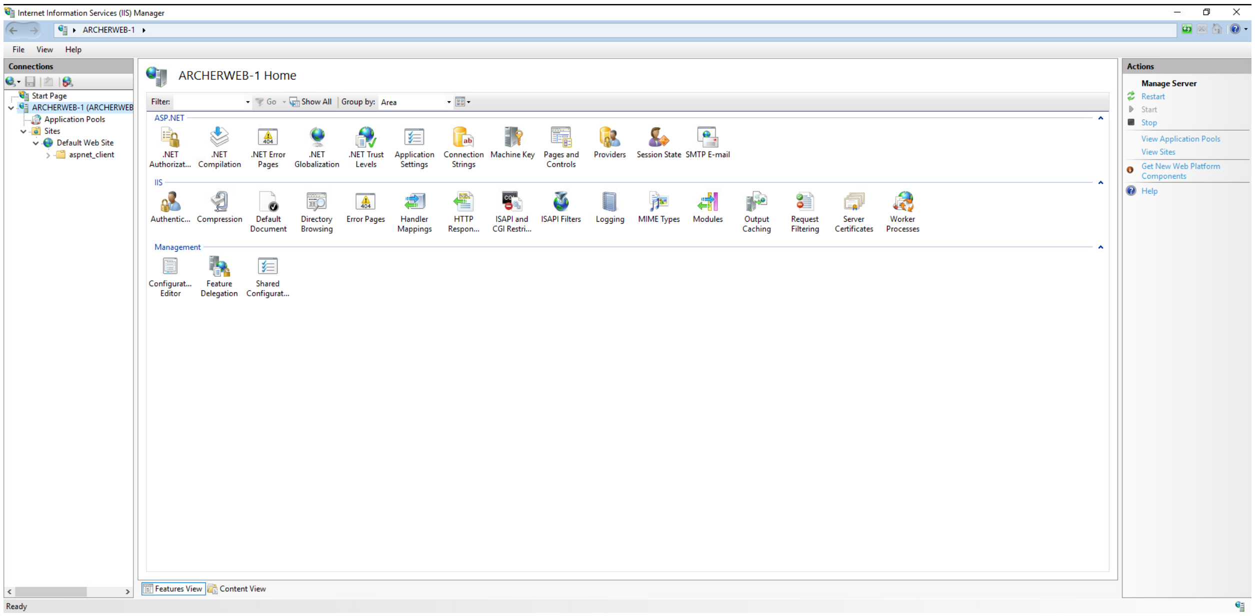
- ☑ Web Server
  - ☑ Common HTTP Features
    - ☑ Default Document
    - ☑ Directory Browsing
    - ☑ HTTP Errors
    - ☑ Static Content
    - □ HTTP Redirection
    - □ WebDAV Publishing
  - ☑ Health and Diagnostics
    - ☑ HTTP Logging
    - □ Custom Logging
    - □ Logging Tools
    - □ ODBC Logging
    - □ Request Monitor
    - □ Tracing
  - ☑ Performance
    - ☑ Static Content Compression
    - ☑ Dynamic Content Compression
  - ☑ Security
    - ☑ Request Filtering
    - □ Basic Authentication
    - □ Centralized SSL Certificate Support
    - □ Client Certificate Mapping Authentication
    - □ Digest Authentication
    - □ IIS Client Certificate Mapping Authentication
    - □ IP and Domain Restrictions
    - □ URL Authorization
    - □ Windows Authentication
  - ☑ Application Development
    - □ .NET Extensibility 3.5
    - ☑ .NET Extensibility 4.6
    - □ Application Initialization
    - □ ASP
    - □ ASP.NET 3.5
    - ☑ ASP.NET 4.6
    - □ CGI
    - ☑ ISAPI Extensions
    - ☑ ISAPI Filters
    - □ Server Side Includes
    - □ WebSocket Protocol
- □ FTP Server
- ☑ Management Tools
  - ☑ IIS Management Console

10. Confirm that the selected options are correct and select **Install.**
11. Once the installation completes, select **Close.**
12. Restart the computer.

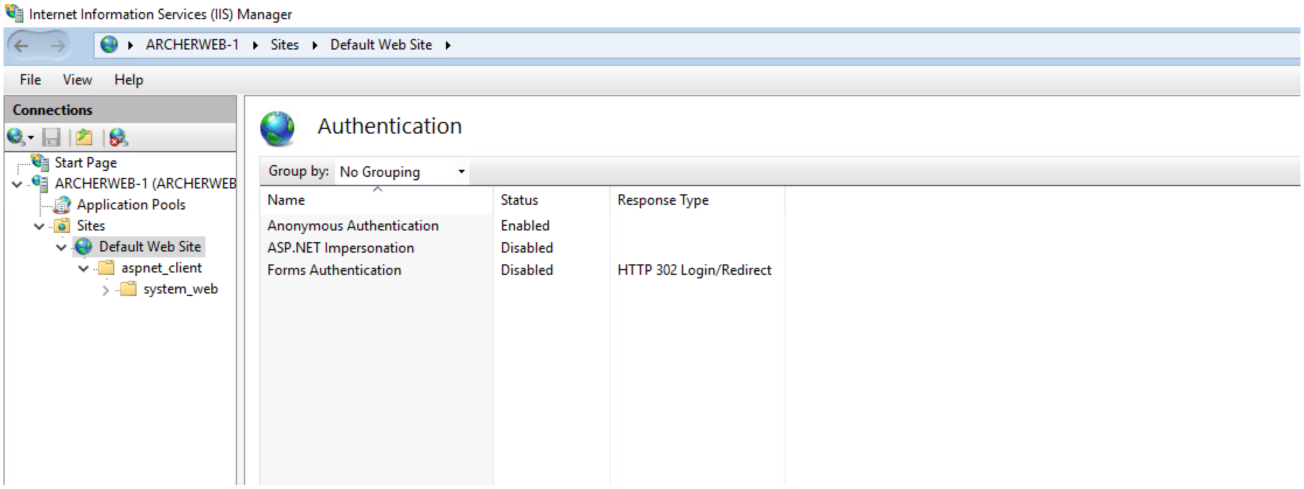
2.8.1.4 Configure IIS

1. Open the IIS application.

2. Click on the web server in the left pane. Select **Authentication**.

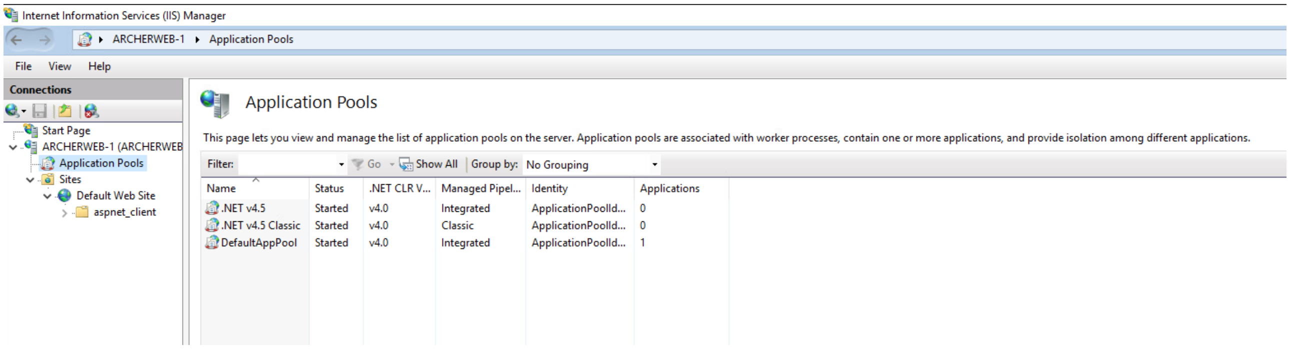


3. Ensure that **Anonymous Authentication** is enabled and **ASP.NET Impersonation** and **Forms Authentication** are disabled for the **Default Web Site**.



Name	Status	Response Type
Anonymous Authentication	Enabled	
ASP.NET Impersonation	Disabled	
Forms Authentication	Disabled	HTTP 302 Login/Redirect

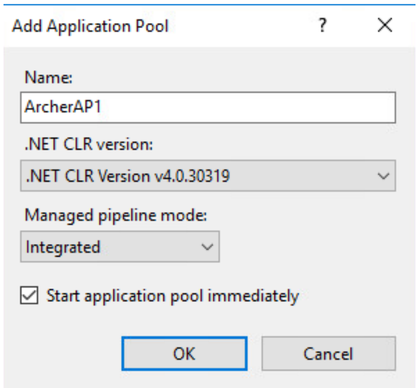
4. Expand the web server tree and select **Application Pools.** In the far-right pane, select **Add Application Pool.**



This page lets you view and manage the list of application pools on the server. Application pools are associated with worker processes, contain one or more applications, and provide isolation among different applications.

Name	Status	.NET CLR V...	Managed Pipel...	Identity	Applications
.NET v4.5	Started	v4.0	Integrated	ApplicationPoolId...	0
.NET v4.5 Classic	Started	v4.0	Classic	ApplicationPoolId...	0
DefaultAppPool	Started	v4.0	Integrated	ApplicationPoolId...	1

5. Add a name to the **Name** input field. Ensure that **Managed pipeline mode** is set to **Integrated** and that **Start application pool immediately** is selected. Then, select **OK**.



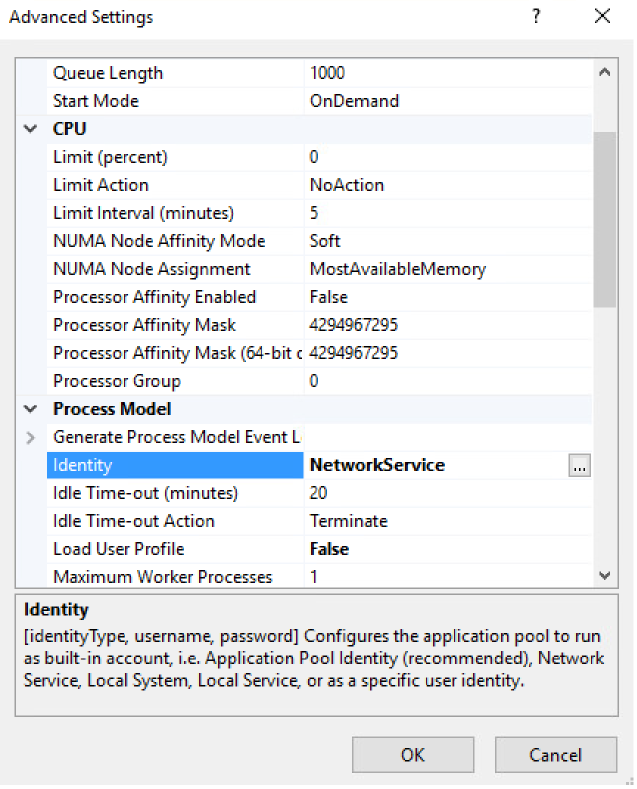
Name: ArcherAP1

.NET CLR version: .NET CLR Version v4.0.30319

Managed pipeline mode: Integrated

☑ Start application pool immediately

6. Right-click on the newly created application pool and select **Advanced Settings**. Under **Process Model,** select the ellipsis button that is next to the **Identity** field.

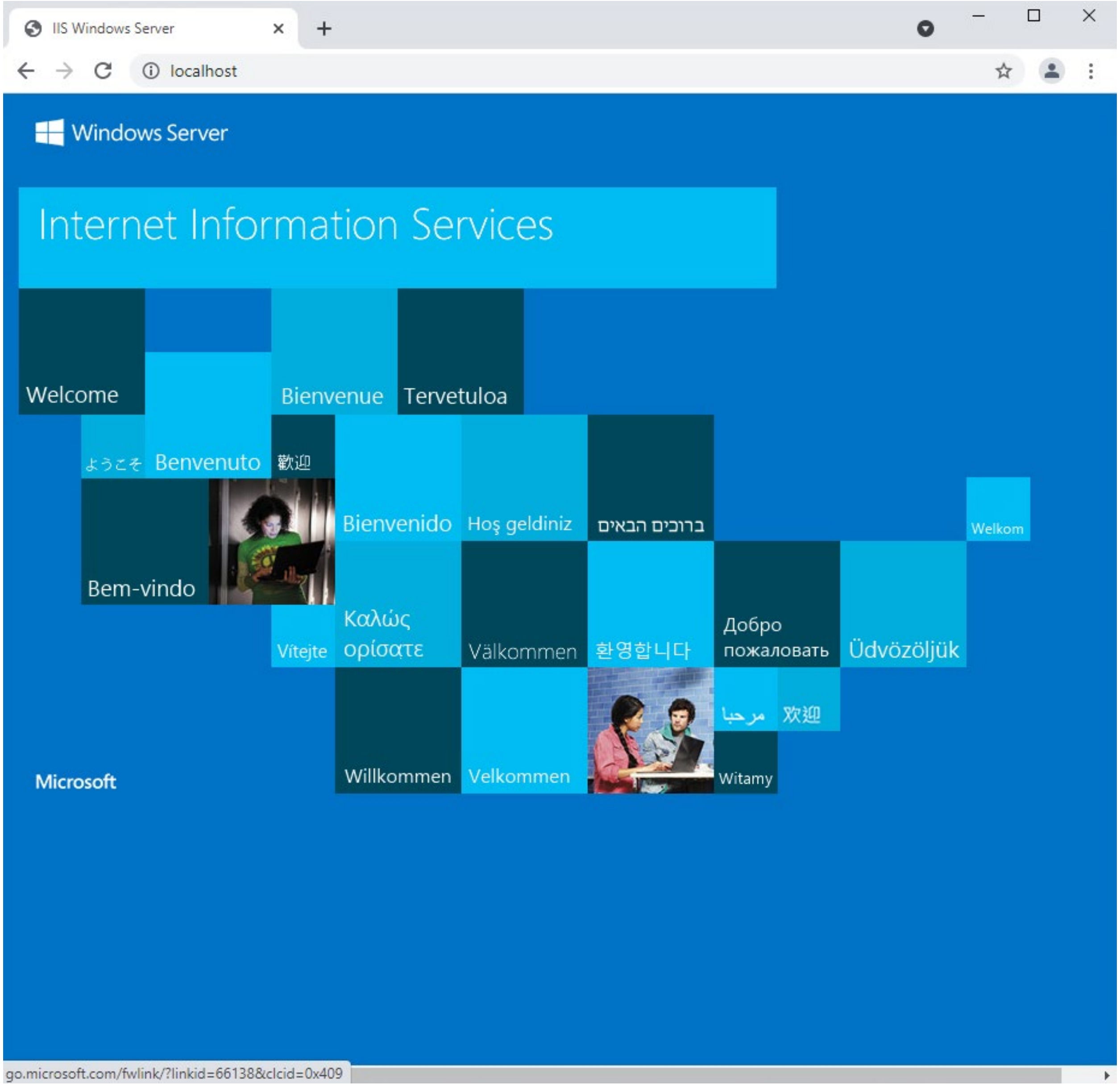


Advanced Settings

Queue Length	1000
Start Mode	OnDemand
CPU	
Limit (percent)	0
Limit Action	NoAction
Limit Interval (minutes)	5
NUMA Node Affinity Mode	Soft
NUMA Node Assignment	MostAvailableMemory
Processor Affinity Enabled	False
Processor Affinity Mask	4294967295
Processor Affinity Mask (64-bit c	4294967295
Processor Group	0
Process Model	
Generate Process Model Event L	
Identity	**NetworkService**
Idle Time-out (minutes)	20
Idle Time-out Action	Terminate
Load User Profile	**False**
Maximum Worker Processes	1

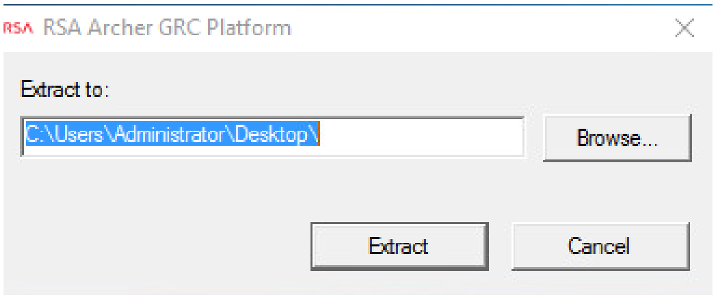
Identity
[identityType, username, password] Configures the application pool to run as built-in account, i.e. Application Pool Identity (recommended), Network Service, Local System, Local Service, or as a specific user identity.

7. Select **Custom account**, select **Set**, and enter the appropriate information. Then select **OK.**
8. Click on the web server. In the far-right pane, select **Restart**.
9. Open a browser and navigate to localhost. If the screen below is shown, then the web server is running properly, and RSA Archer can now be installed.



2.8.2 RSA Archer Installation

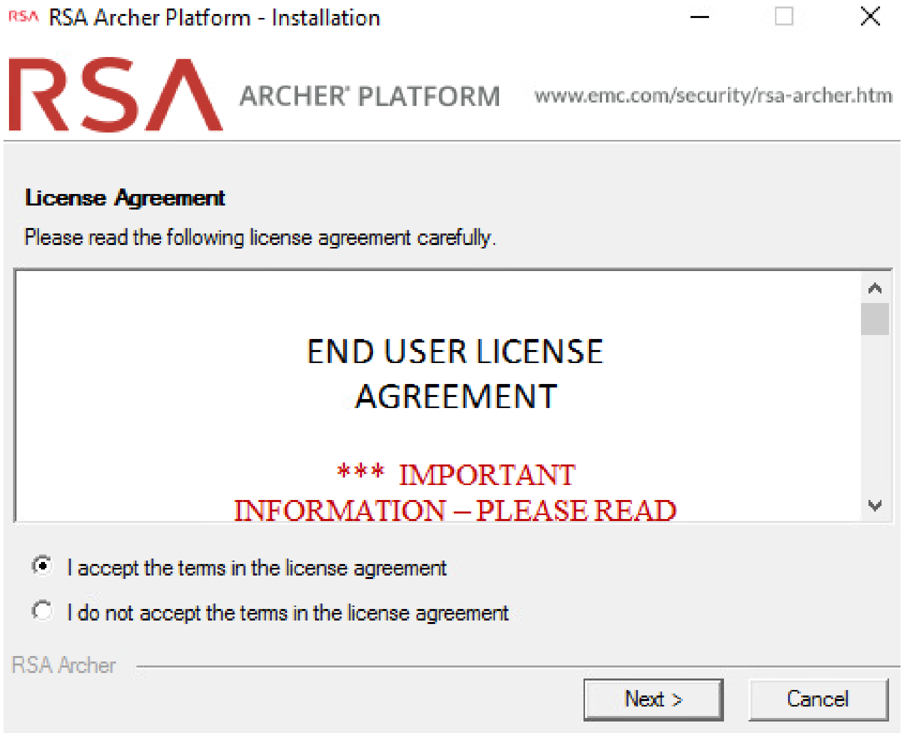
1. Before installing RSA Archer, .NET Framework version 4.7.2 must be installed. It can be downloaded at https://dotnet.microsoft.com/download/dotnet-framework/net472.
2. Extract the zip file that was downloaded from the RSA Archer download page.



RSA Archer GRC Platform

Extract to: C:\Users\Administrator\Desktop\

3. Open the folder and run the executable **ArcherInstall.**
4. Accept the License Agreement and select **Next.**



RSA Archer Platform - Installation

RSA ARCHER® PLATFORM www.emc.com/security/rsa-archer.htm

License Agreement

Please read the following license agreement carefully.

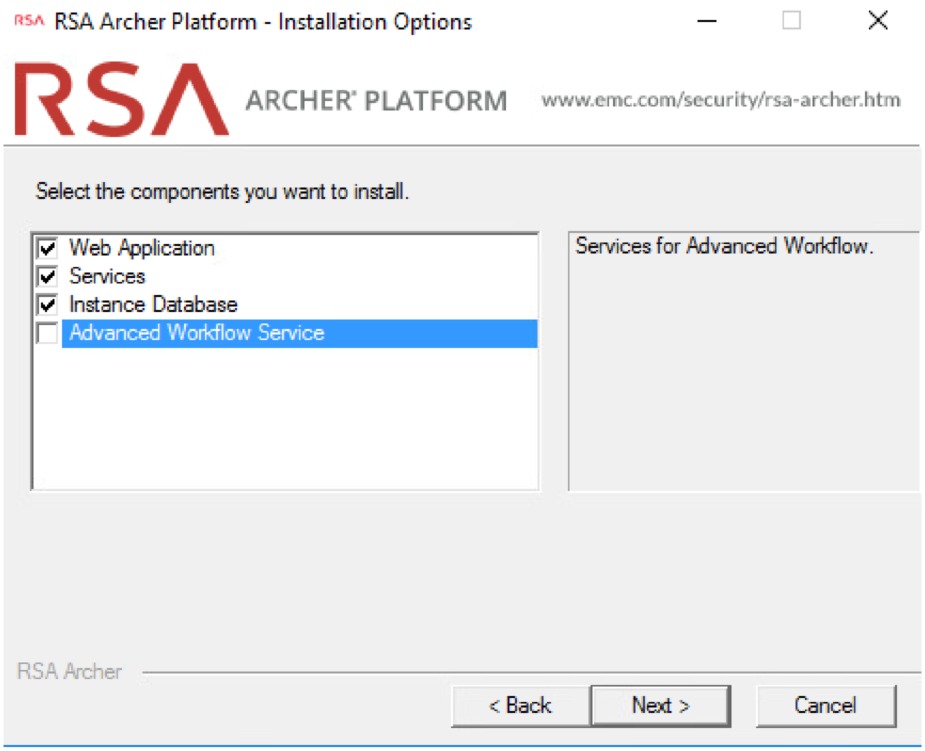
END USER LICENSE AGREEMENT

*** IMPORTANT INFORMATION – PLEASE READ

● I accept the terms in the license agreement

○ I do not accept the terms in the license agreement

5. Select **Next.**
6. For the web server, make sure the components **Web Application**, **Services**, and **Instance Database** are selected, then select **Next.**

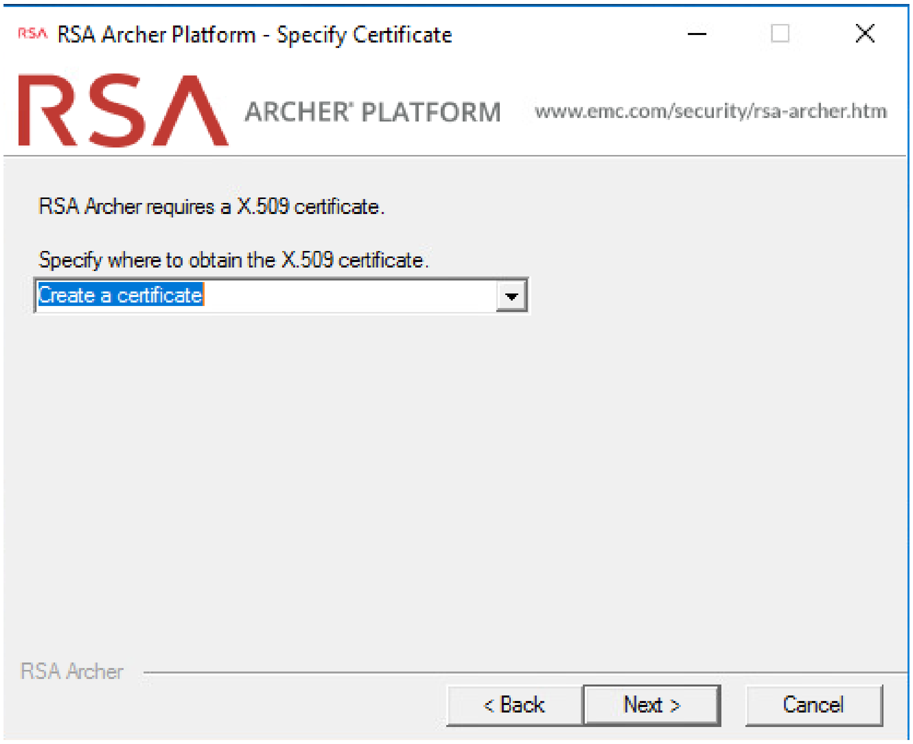

RSA Archer Platform - Installation Options
RSA
ARCHER® PLATFORM
www.emc.com/security/rsa-archer.htm
RSA Archer
< Back
Next >
Cancel

Select the components you want to install.

- ☑ Web Application
- ☑ Services
- ☑ Instance Database
- □ Advanced Workflow Service

Services for Advanced Workflow.

7. Select **Create a certificate** from the dropdown menu and select **Next.**


RSA Archer Platform - Specify Certificate
RSA ARCHER® PLATFORM
www.emc.com/security/rsa-archer.htm

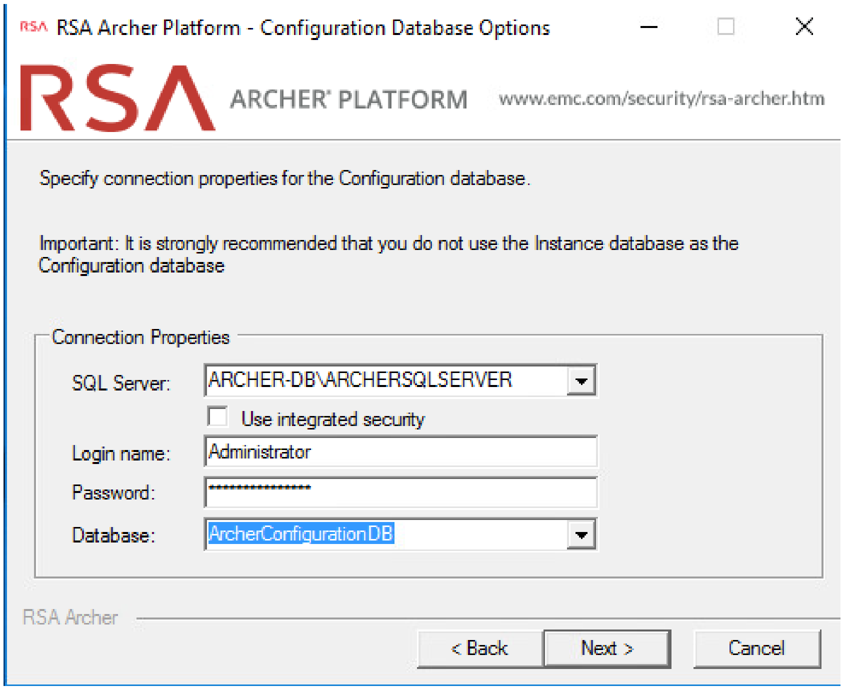
RSA Archer requires a X.509 certificate.

Specify where to obtain the X.509 certificate.

Create a certificate

RSA Archer
< Back
Next >
Cancel

8. Select the database server that was previously created. Enter the credentials that were created in SSMS. Then select the configuration database from the dropdown menu, and click **Next**.


RSA Archer Platform - Configuration Database Options
RSA ARCHER® PLATFORM
www.emc.com/security/rsa-archer.htm

Specify connection properties for the Configuration database.

Important: It is strongly recommended that you do not use the Instance database as the Configuration database

Connection Properties

SQL Server: ARCHER-DB\ARCHERSQLSERVER

□ Use integrated security

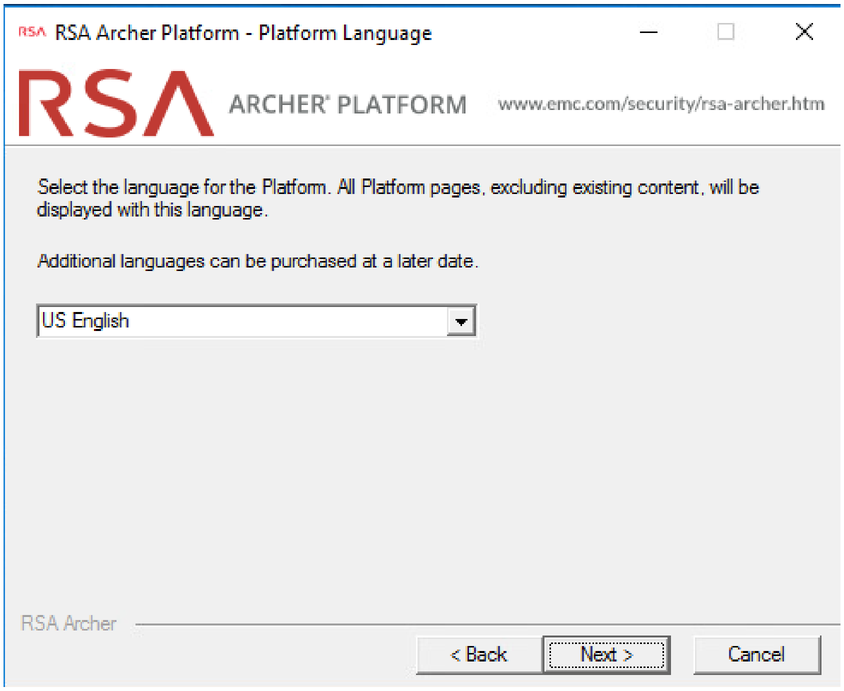
Login name: Administrator

Password: ****************

Database: ArcherConfigurationDB

RSA Archer
< Back
Next >
Cancel

9. Select the preferred language from the dropdown menu and select **Next.**



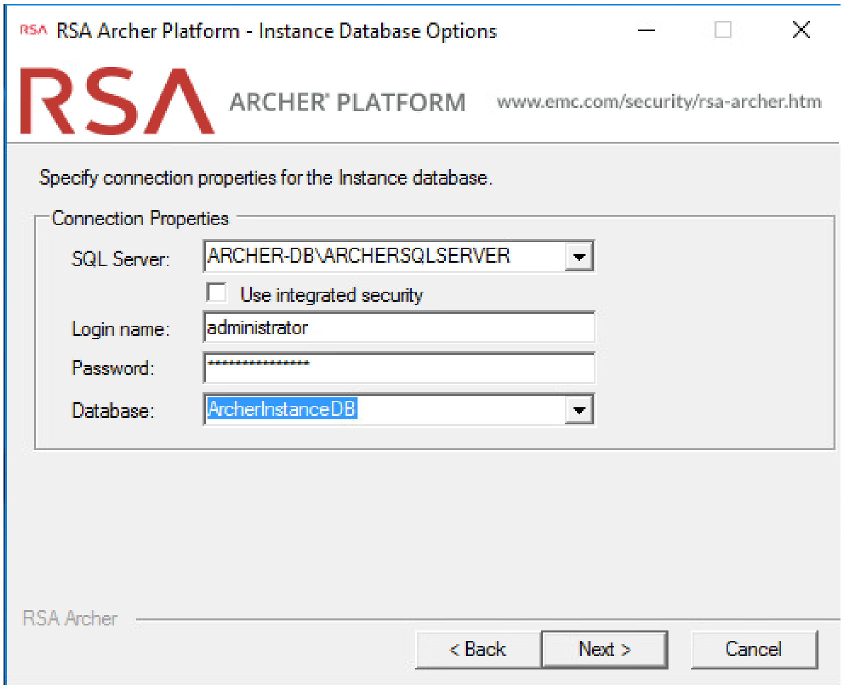
RSA Archer Platform - Platform Language

Select the language for the Platform. All Platform pages, excluding existing content, will be displayed with this language.

Additional languages can be purchased at a later date.

US English

10. Repeat step 8 and select the instance database from the dropdown menu. Then select **Next.**



RSA Archer Platform - Instance Database Options

Specify connection properties for the Instance database.

Connection Properties

SQL Server: ARCHER-DB\ARCHERSQLSERVER

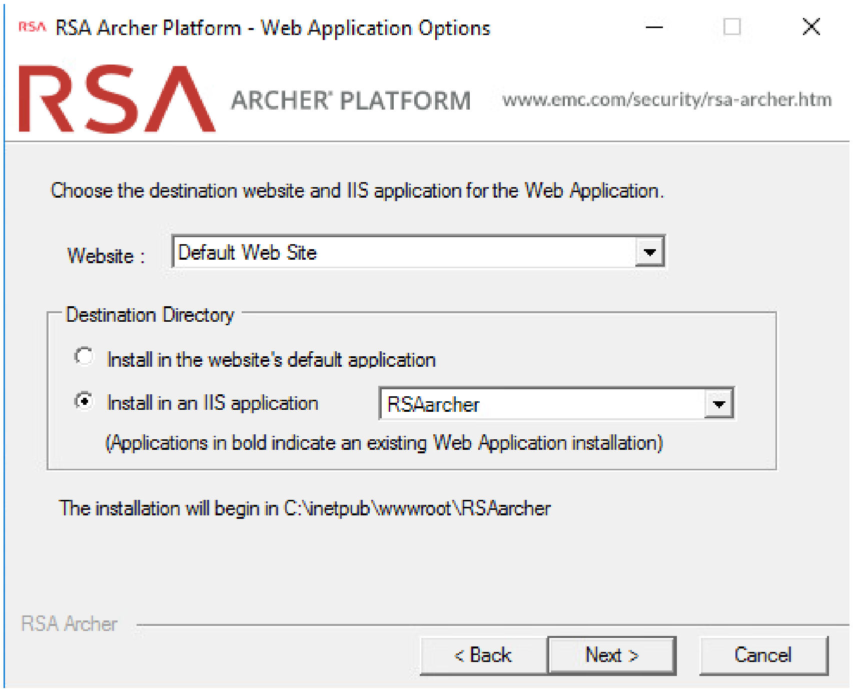
□ Use integrated security

Login name: administrator

Password: ****************

Database: ArcherInstanceDB

11. Select the time zone and select **Next.**
12. Select **Default Web Site** as the website location and choose the **Install an IIS application** radio button. Select **RSAarcher** from the dropdown menu. Then select **Next.**


RSA Archer Platform - Web Application Options
RSA
ARCHER PLATFORM
www.emc.com/security/rsa-archer.htm

Choose the destination website and IIS application for the Web Application.

Website : Default Web Site

Destination Directory

○ Install in the website's default application

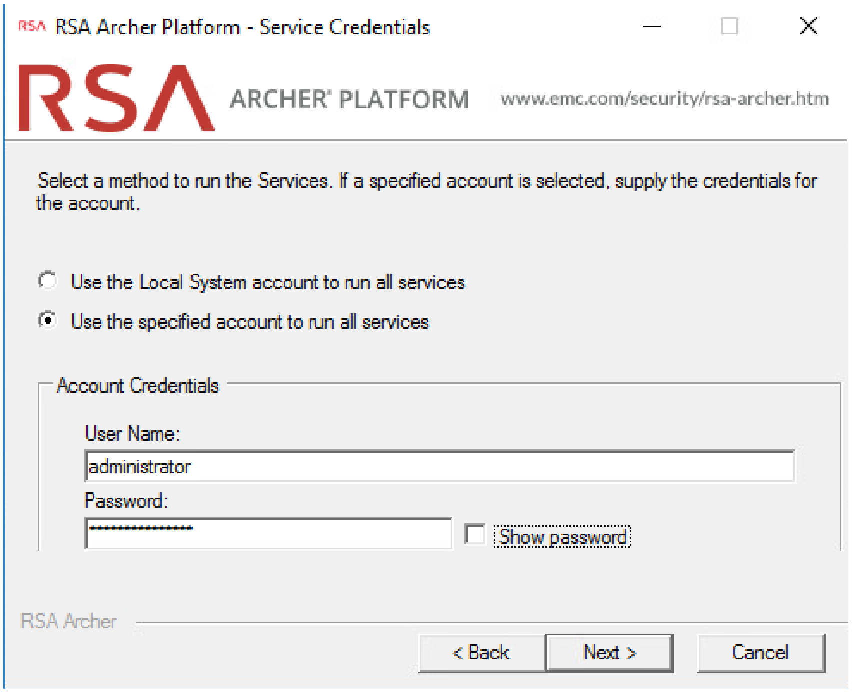
● Install in an IIS application RSAarcher

(Applications in bold indicate an existing Web Application installation)

The installation will begin in C:\inetpub\wwwroot\RSAarcher

RSA Archer
< Back
Next >
Cancel

13. To add an Instrumentation Database, repeat step 8 and use the **ArcherLogging** database that was created in SSMS. Otherwise, select **Not using RSA Archer Instrumentation service**. Select **Next**.
14. Specify the account to run the services. Then select **Next**.



RSA Archer Platform - Service Credentials

RSA ARCHER® PLATFORM www.emc.com/security/rsa-archer.htm

Select a method to run the Services. If a specified account is selected, supply the credentials for the account.

○ Use the Local System account to run all services

● Use the specified account to run all services

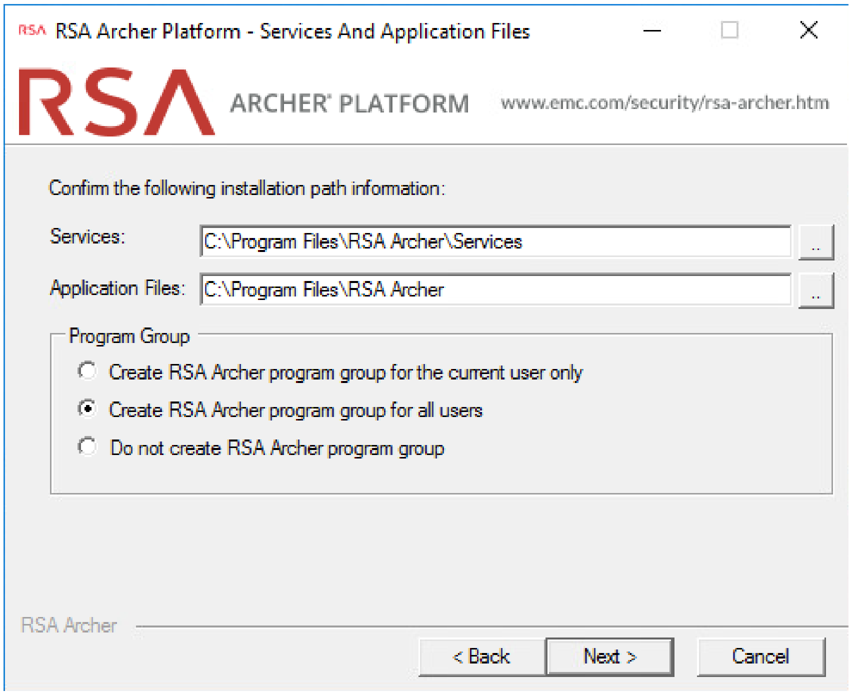
Account Credentials

User Name: administrator

Password: ****************

□ Show password

15. Confirm or edit the installation paths for the services and application files. Select the **Create RSA Archer program group for all users** radio button. Then select **Next**.



RSA Archer Platform - Services And Application Files

RSA ARCHER® PLATFORM www.emc.com/security/rsa-archer.htm

Confirm the following installation path information:

Services: C:\Program Files\RSA Archer\Services

Application Files: C:\Program Files\RSA Archer

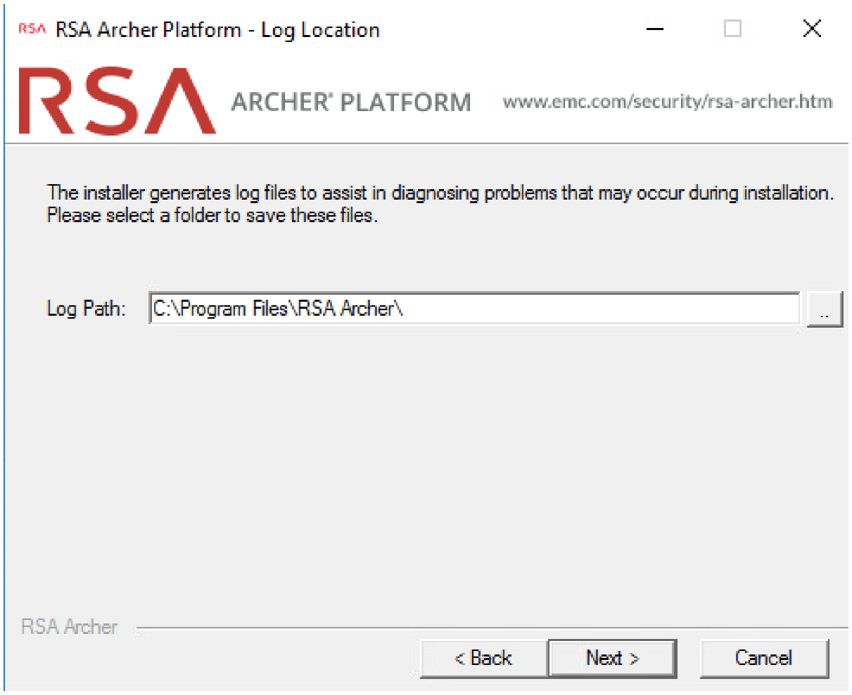
Program Group

○ Create RSA Archer program group for the current user only

● Create RSA Archer program group for all users

○ Do not create RSA Archer program group

677 16. Confirm or edit the path for installation logs. Then select **Next.**



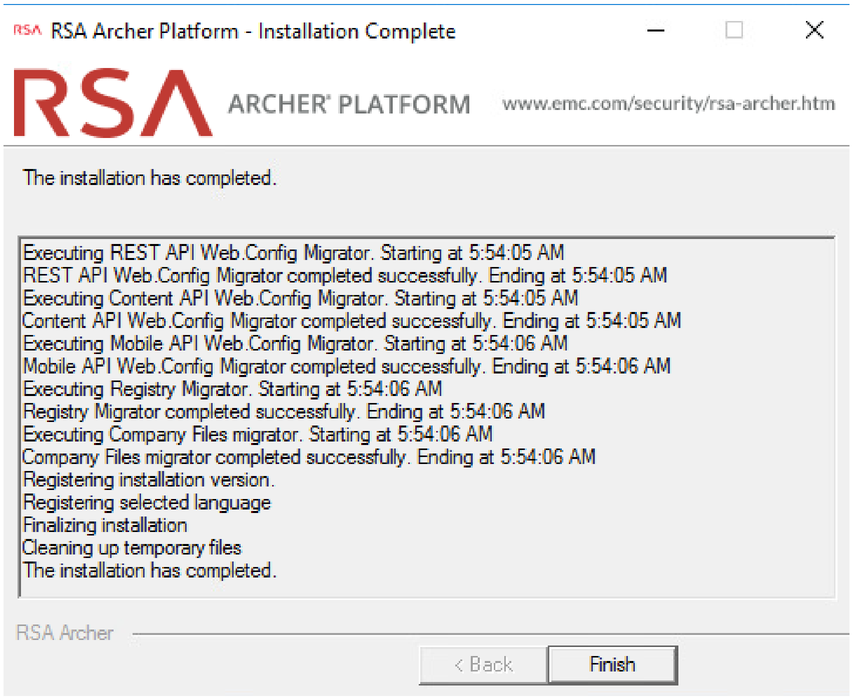
RSA Archer Platform - Log Location

The installer generates log files to assist in diagnosing problems that may occur during installation. Please select a folder to save these files.

Log Path: C:\Program Files\RSA Archer\

678

679 17. Select **Install** and wait for the installation to complete. Once completed, select **Finish.**



RSA Archer Platform - Installation Complete

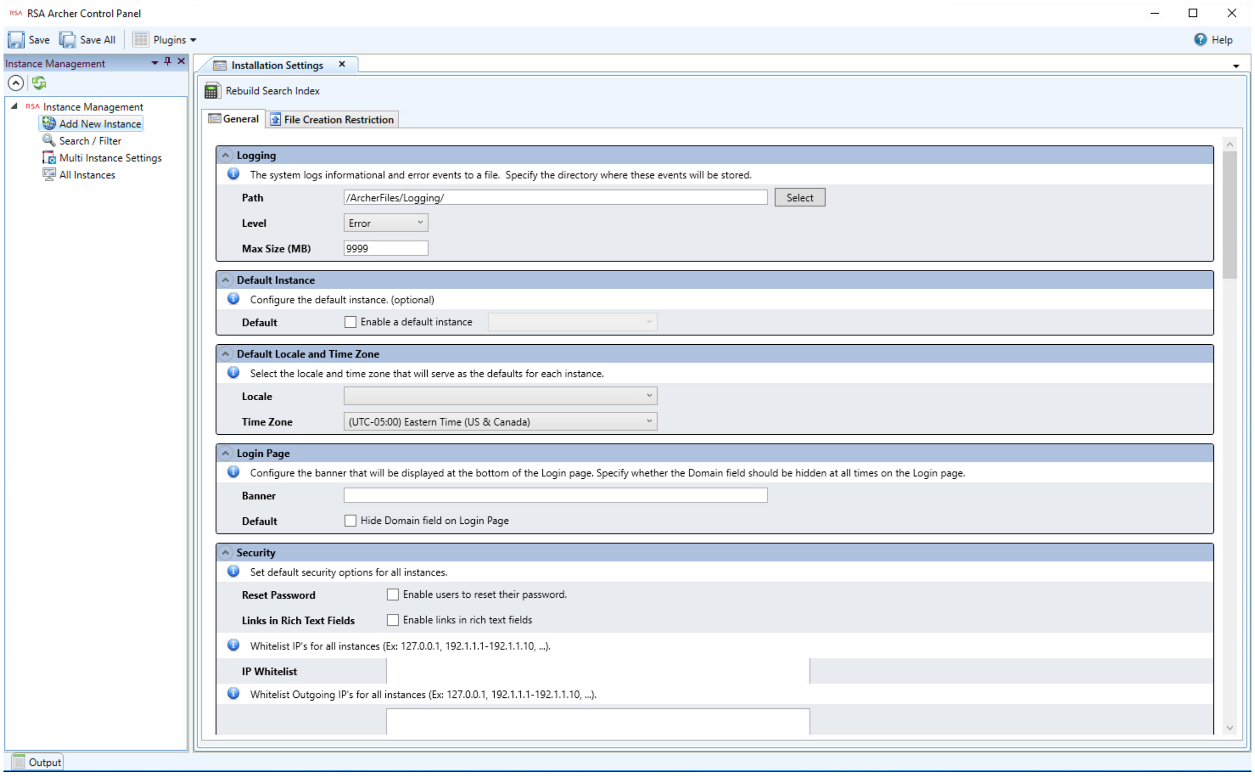
The installation has completed.

```
Executing REST API Web.Config Migrator. Starting at 5:54:05 AM
REST API Web.Config Migrator completed successfully. Ending at 5:54:05 AM
Executing Content API Web.Config Migrator. Starting at 5:54:05 AM
Content API Web.Config Migrator completed successfully. Ending at 5:54:05 AM
Executing Mobile API Web.Config Migrator. Starting at 5:54:06 AM
Mobile API Web.Config Migrator completed successfully. Ending at 5:54:06 AM
Executing Registry Migrator. Starting at 5:54:06 AM
Registry Migrator completed successfully. Ending at 5:54:06 AM
Executing Company Files migrator. Starting at 5:54:06 AM
Company Files migrator completed successfully. Ending at 5:54:06 AM
Registering installation version.
Registering selected language
Finalizing installation
Cleaning up temporary files
The installation has completed.
```

680

2.8.2.1 Configure Options in the Control Panel

1. Open the RSA Control Panel.
2. In the left pane, select **Add New Instance.**



Logging
The system logs informational and error events to a file. Specify the directory where these events will be stored.
Path: /ArcherFiles/Logging/ [Select]
Level: Error
Max Size (MB): 9999

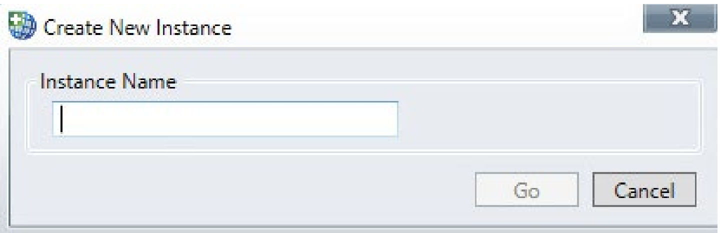
Default Instance
Configure the default instance. (optional)
Default: □ Enable a default instance

Default Locale and Time Zone
Select the locale and time zone that will serve as the defaults for each instance.
Locale:
Time Zone: (UTC-05:00) Eastern Time (US & Canada)

Login Page
Configure the banner that will be displayed at the bottom of the Login page. Specify whether the Domain field should be hidden at all times on the Login page.
Banner:
Default: □ Hide Domain field on Login Page

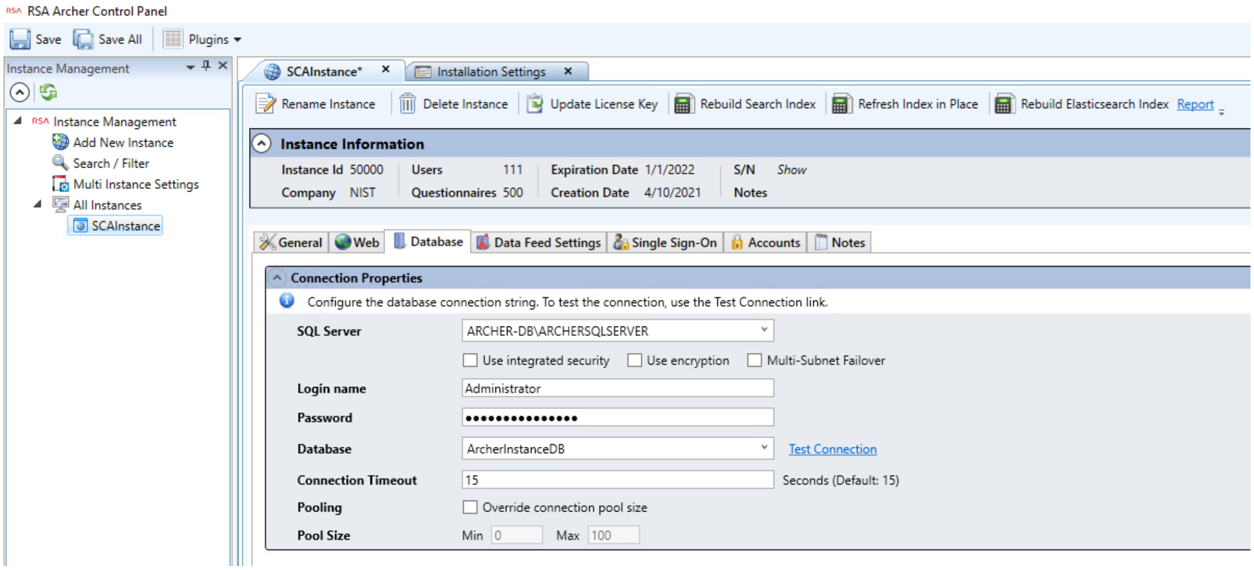
Security
Set default security options for all instances.
Reset Password: □ Enable users to reset their password.
Links in Rich Text Fields: □ Enable links in rich text fields
Whitelist IP's for all instances (Ex: 127.0.0.1, 192.1.1.1-192.1.1.10, ...).
IP Whitelist:
Whitelist Outgoing IP's for all instances (Ex: 127.0.0.1, 192.1.1.1-192.1.1.10, ...).

3. Enter a name for the instance in the **Instance Name** field. Select **Go.**



Instance Name:

4. Double-click on the new instance. Input the required information in the **General**, **Web**, and **Database** tabs. When completed, click **Save** in the top left corner.



Instance Information

Instance Id	50000	Users	111	Expiration Date	1/1/2022	S/N	Show
Company	NIST	Questionnaires	500	Creation Date	4/10/2021	Notes	

Connection Properties

Configure the database connection string. To test the connection, use the Test Connection link.

SQL Server: ARCHER-DB\ARCHERSQLSERVER

□ Use integrated security □ Use encryption □ Multi-Subnet Failover

Login name: Administrator

Password: •••••••••••••••

Database: ArcherInstanceDB

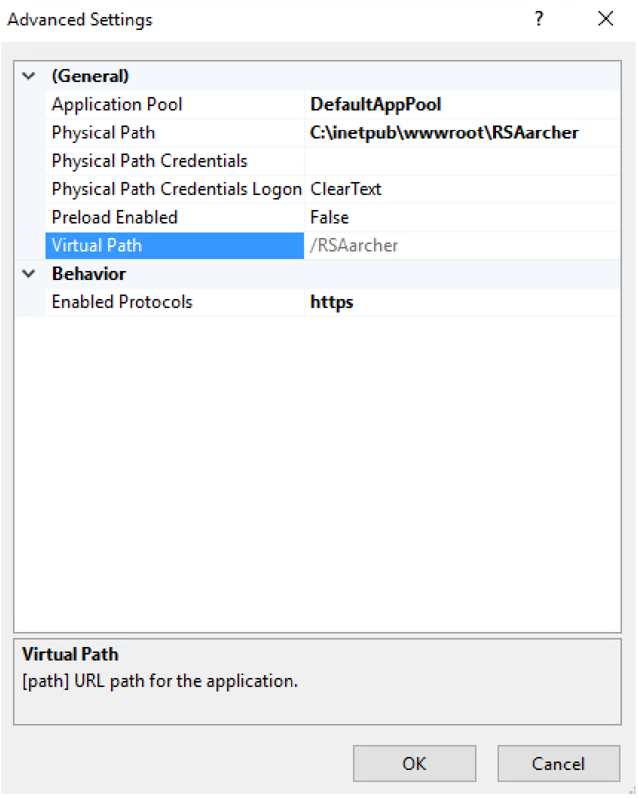
Connection Timeout: 15 Seconds (Default: 15)

Pooling: □ Override connection pool size

Pool Size: Min 0 Max 100

2.8.2.2 Add New Application to Application Pool

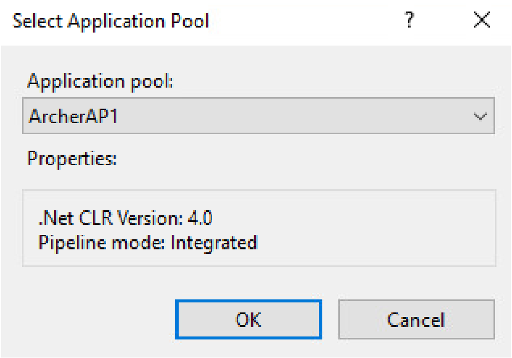
1. Navigate back to IIS. Expand the web server directory, expand the **Sites** directory, and expand the **Default Web Site** directory.
2. Select the RSAarcher site. Click on **Authentication** and ensure that **Anonymous Authentication** is the only thing that is enabled.
3. Right-click on the RSAarcher site and select **Manage Application > Advanced Settings.**
4. Click on **Application Pool** and select the ellipsis button. You will see a screen similar to the following:



(General)	
Application Pool	**DefaultAppPool**
Physical Path	**C:\inetpub\wwwroot\RSAarcher**
Physical Path Credentials	
Physical Path Credentials Logon	ClearText
Preload Enabled	False
Virtual Path	/RSAarcher
Behavior	
Enabled Protocols	**https**

Virtual Path
[path] URL path for the application.

5. Select the application pool that was previously created and select **OK**.

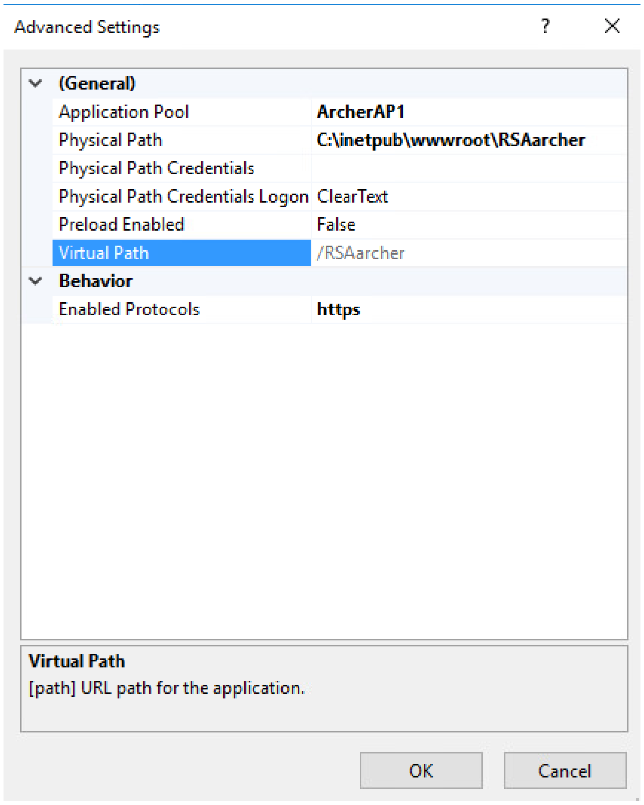


Application pool: ArcherAP1

Properties:

.Net CLR Version: 4.0
Pipeline mode: Integrated

6. Select **OK.** You should see something similar to the screenshot below:



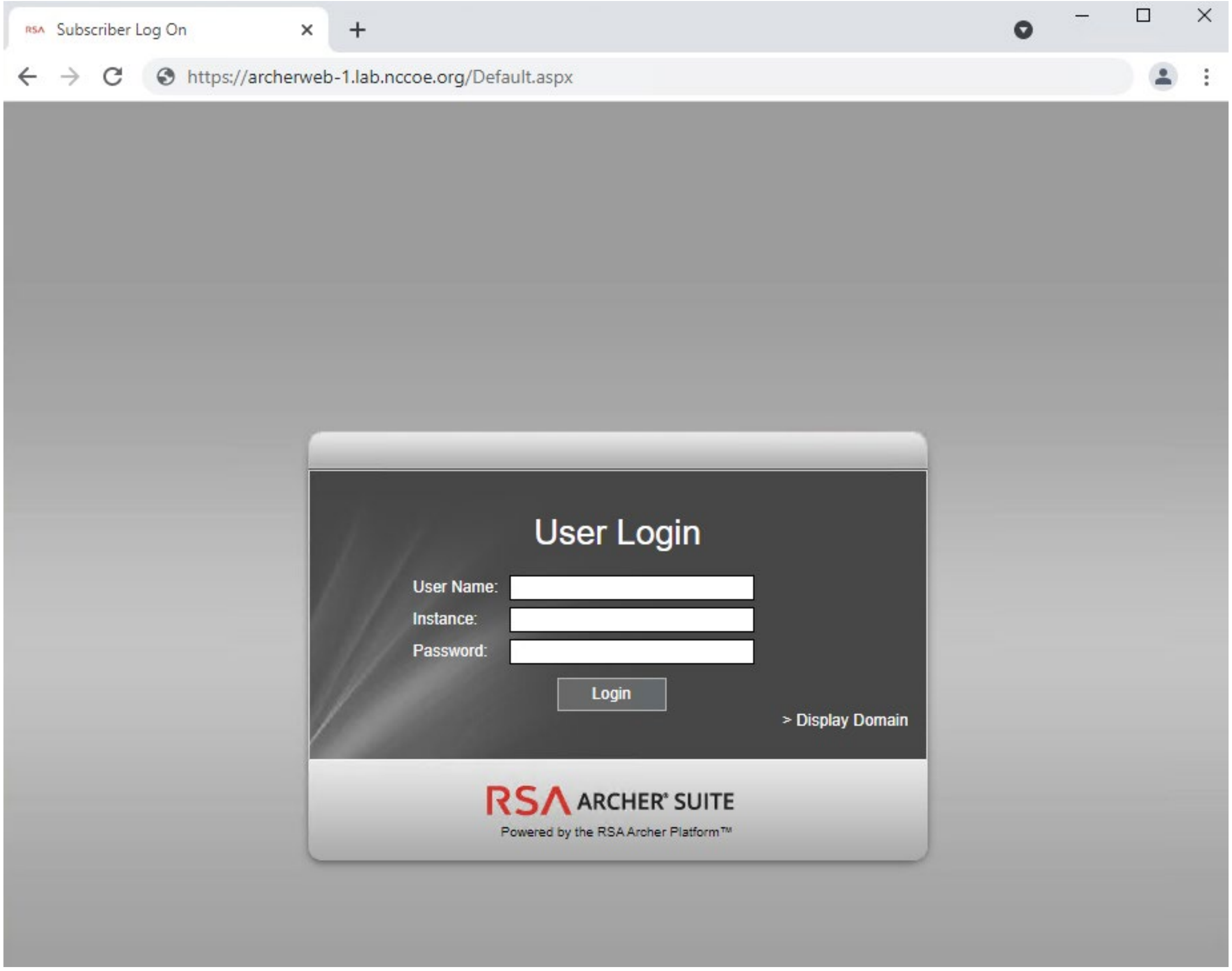
Advanced Settings

(General)	
Application Pool	**ArcherAP1**
Physical Path	**C:\inetpub\wwwroot\RSAarcher**
Physical Path Credentials	
Physical Path Credentials Logon	ClearText
Preload Enabled	False
Virtual Path	/RSAarcher
Behavior	
Enabled Protocols	**https**

Virtual Path
[path] URL path for the application.

7. Restart the RSA Archer site.

8. Open a browser and navigate to the URL that was set in the RSA Control Panel application. If the following page displays, then RSA Archer installed successfully.



2.9 Seagate

This section will be updated to address Seagate storage drives in an updated version of this publication.

2.10 Integrations

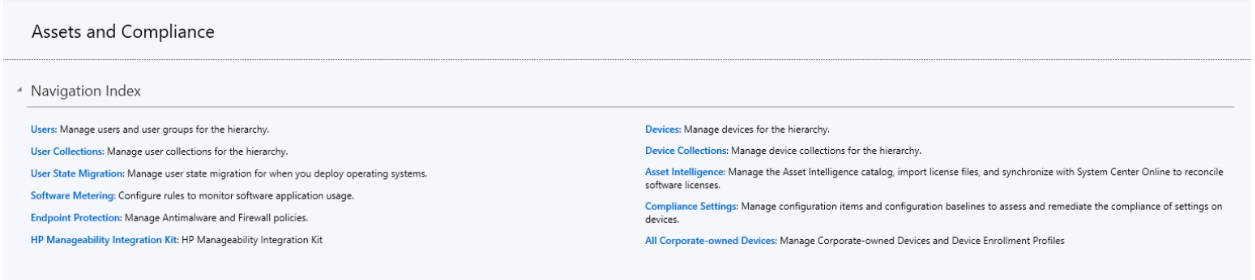
This section describes the steps we took to configure and integrate the products described earlier in this volume. The integrations are generally network-based and require connectivity both between the systems and to Internet-based cloud services.

2.10.1 Microsoft Endpoint Configuration Manager and Intel TSC Tooling

For the Intel laptops, a command-line version of the AutoVerify tool named TSCVerifyUtil periodically monitors the changes to laptop components. A custom PowerShell script installed on each laptop and run every hour via task scheduler captures the result of TSCVerifyUtil execution and stores it in the Windows registry. This section describes how to configure Microsoft Endpoint Configuration Manager to run a configuration baseline which monitors the results of the customized PowerShell script. This data is reflected in the RSA Archer dashboard.

2.10.1.1 Set Up Configuration Item

1. In the Microsoft Endpoint Configuration Manager console, under **Assets and Compliance > Overview**, select **Compliance Settings**.



Assets and Compliance

Navigation Index

Users: Manage users and user groups for the hierarchy.

User Collections: Manage user collections for the hierarchy.

User State Migration: Manage user state migration for when you deploy operating systems.

Software Metering: Configure rules to monitor software application usage.

Endpoint Protection: Manage Antimalware and Firewall policies.

HP Manageability Integration Kit: HP Manageability Integration Kit

Devices: Manage devices for the hierarchy.

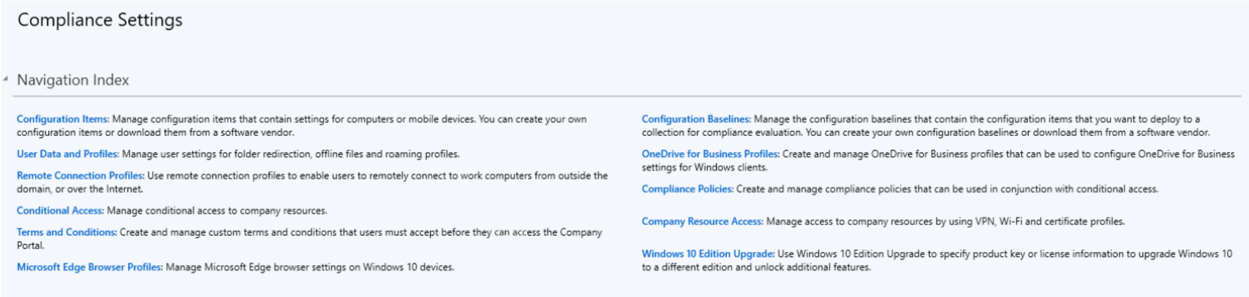
Device Collections: Manage device collections for the hierarchy.

Asset Intelligence: Manage the Asset Intelligence catalog, import license files, and synchronize with System Center Online to reconcile software licenses.

Compliance Settings: Manage configuration items and configuration baselines to assess and remediate the compliance of settings on devices.

All Corporate-owned Devices: Manage Corporate-owned Devices and Device Enrollment Profiles

2. Next, select **Configuration Items**.



Compliance Settings

Navigation Index

Configuration Items: Manage configuration items that contain settings for computers or mobile devices. You can create your own configuration items or download them from a software vendor.

User Data and Profiles: Manage user settings for folder redirection, offline files and roaming profiles.

Remote Connection Profiles: Use remote connection profiles to enable users to remotely connect to work computers from outside the domain, or over the Internet.

Conditional Access: Manage conditional access to company resources.

Terms and Conditions: Create and manage custom terms and conditions that users must accept before they can access the Company Portal.

Microsoft Edge Browser Profiles: Manage Microsoft Edge browser settings on Windows 10 devices.

Configuration Baselines: Manage the configuration baselines that contain the configuration items that you want to deploy to a collection for compliance evaluation. You can create your own configuration baselines or download them from a software vendor.

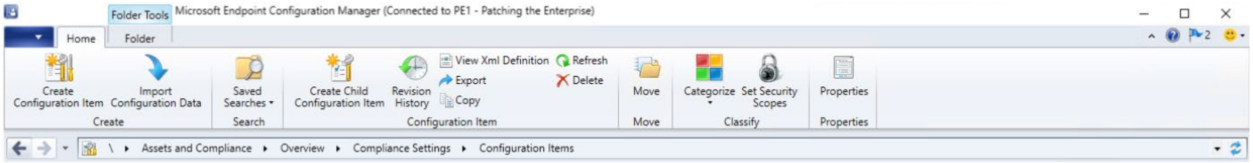
OneDrive for Business Profiles: Create and manage OneDrive for Business profiles that can be used to configure OneDrive for Business settings for Windows clients.

Compliance Policies: Create and manage compliance policies that can be used in conjunction with conditional access.

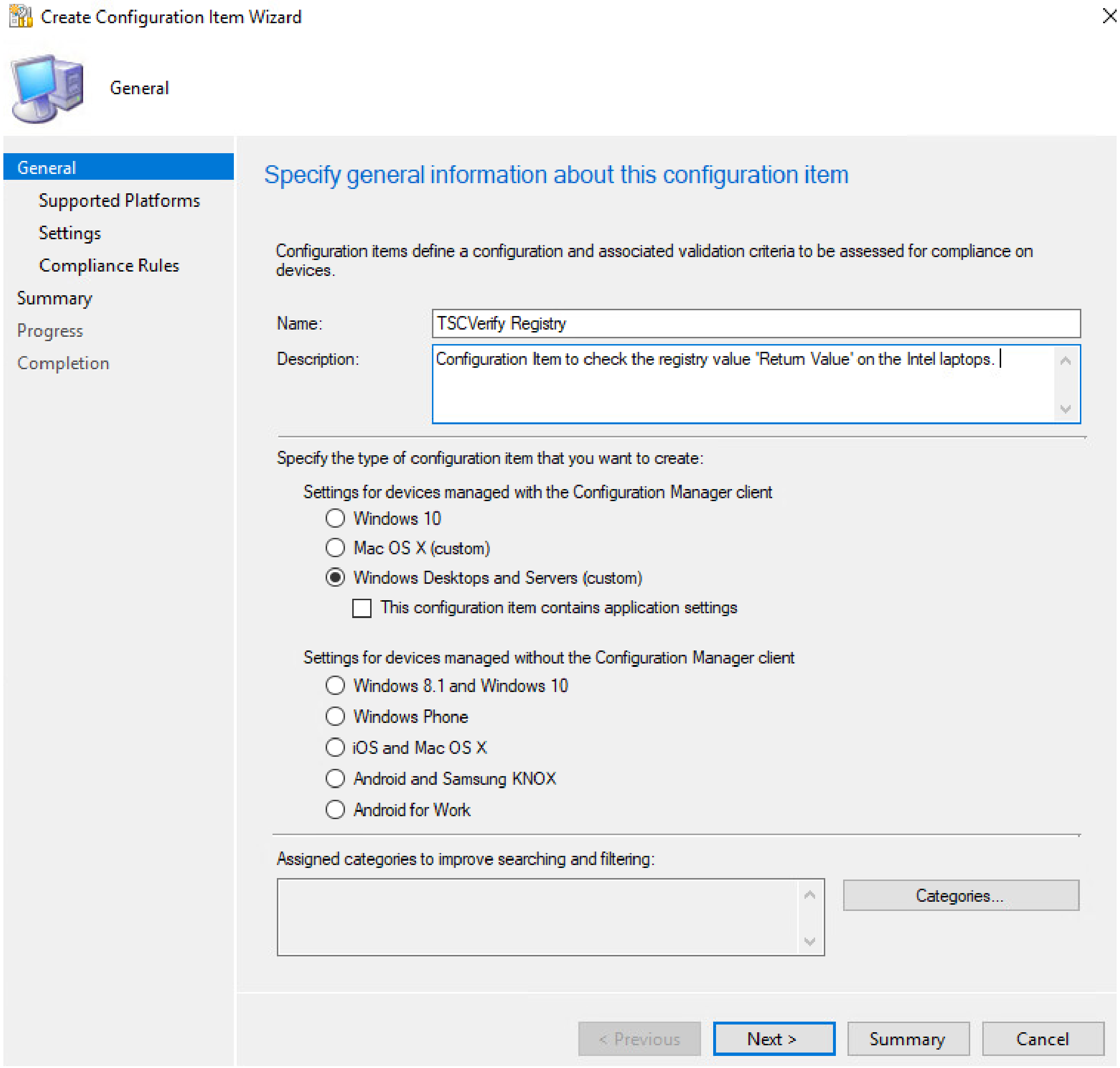
Company Resource Access: Manage access to company resources by using VPN, Wi-Fi and certificate profiles.

Windows 10 Edition Upgrade: Use Windows 10 Edition Upgrade to specify product key or license information to upgrade Windows 10 to a different edition and unlock additional features.

3. From the **Home** panel at the top, select **Create Configuration Item**.



4. Enter a name and description for the configuration item in the **Name** and **Description** fields. Ensure that **Windows Desktops and Servers (custom)** is selected. Then select **Next.**



Create Configuration Item Wizard

General

Specify general information about this configuration item

Configuration items define a configuration and associated validation criteria to be assessed for compliance on devices.

Name: TSCVerify Registry

Description: Configuration Item to check the registry value 'Return Value' on the Intel laptops.

Specify the type of configuration item that you want to create:

Settings for devices managed with the Configuration Manager client

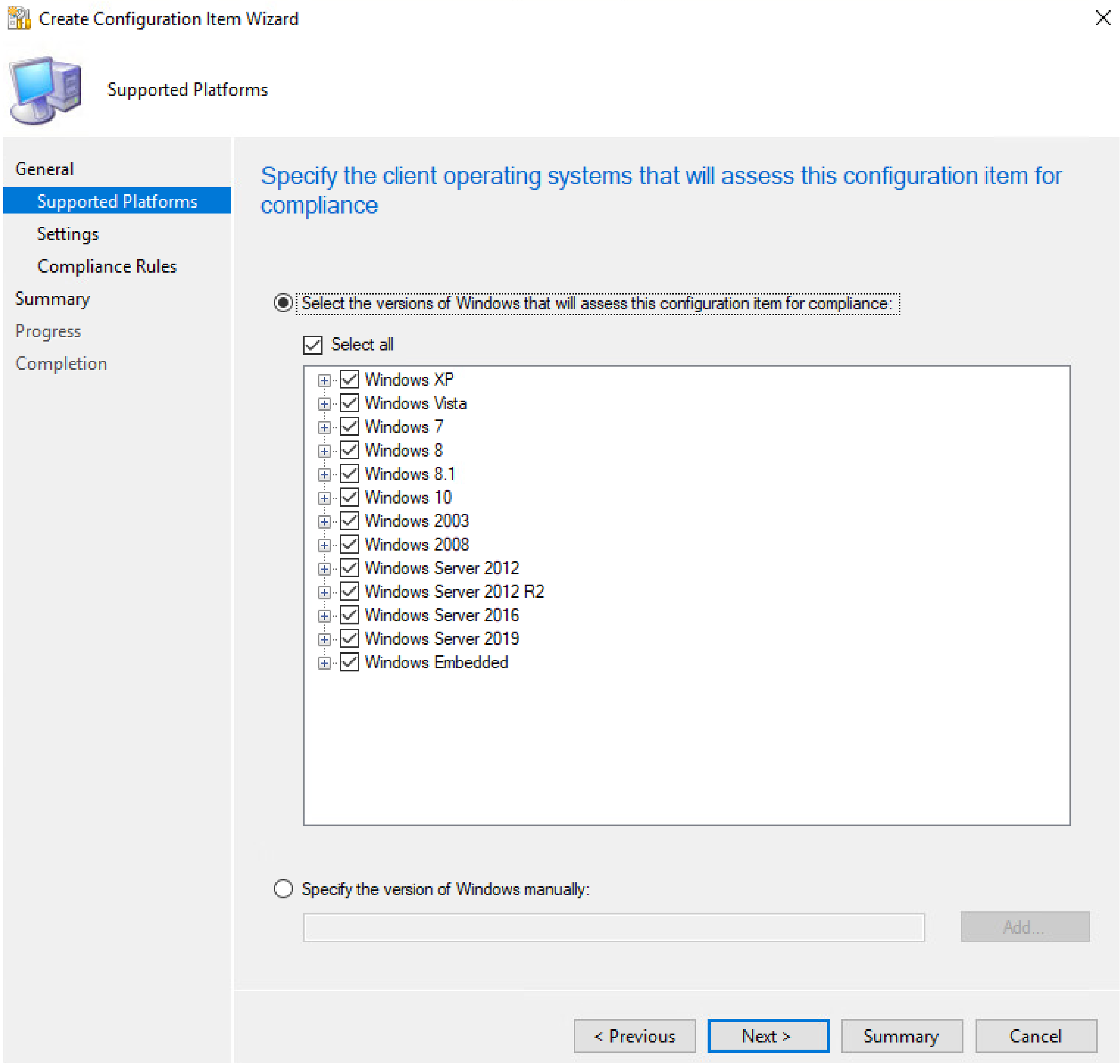
○ Windows 10
○ Mac OS X (custom)
● Windows Desktops and Servers (custom)
□ This configuration item contains application settings

Settings for devices managed without the Configuration Manager client

○ Windows 8.1 and Windows 10
○ Windows Phone
○ iOS and Mac OS X
○ Android and Samsung KNOX
○ Android for Work

Assigned categories to improve searching and filtering:

5. Ensure that all versions are selected and click **Next.**



Specify the client operating systems that will assess this configuration item for compliance

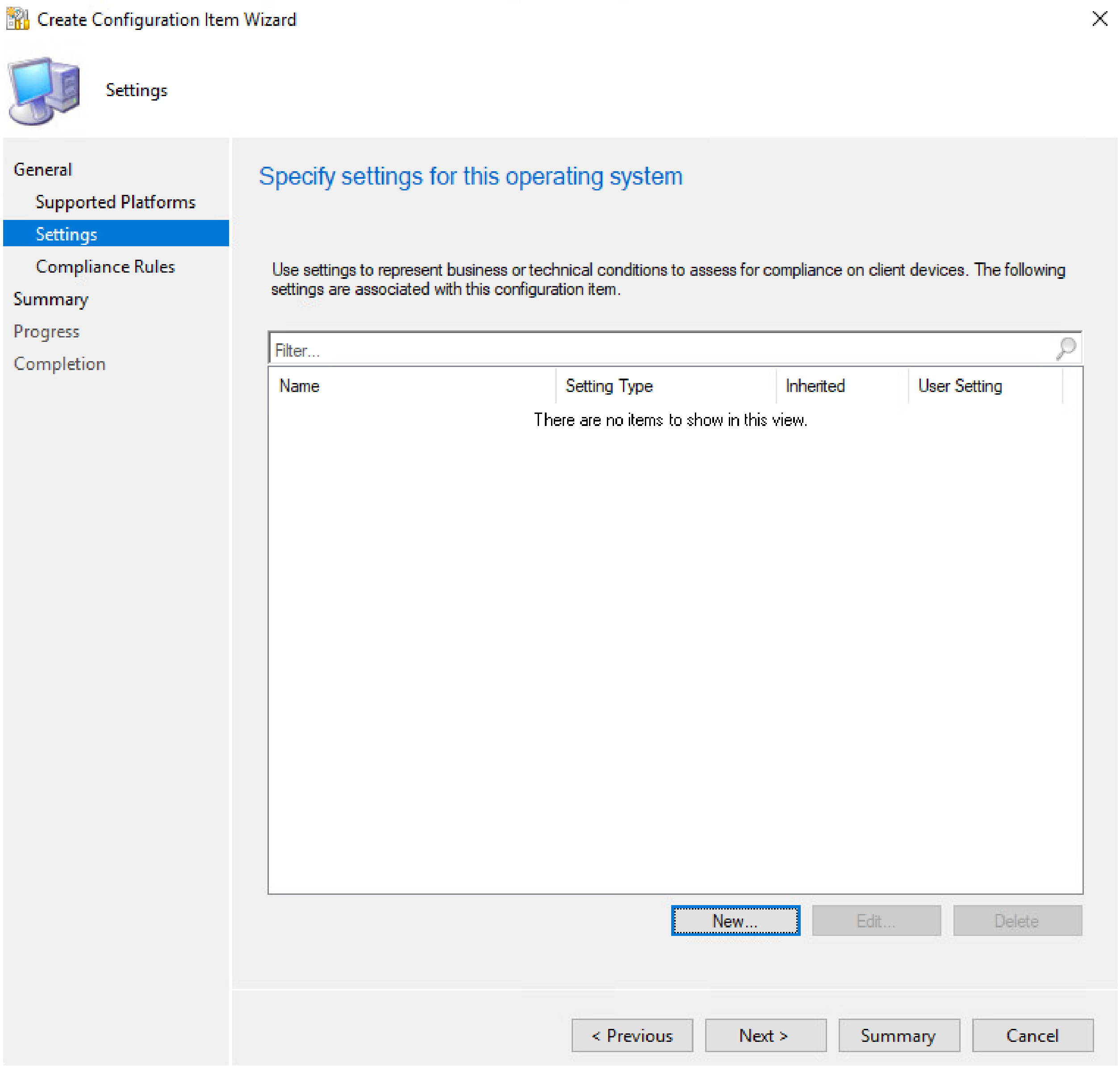
● Select the versions of Windows that will assess this configuration item for compliance:

☑ Select all

- ☑ Windows XP
- ☑ Windows Vista
- ☑ Windows 7
- ☑ Windows 8
- ☑ Windows 8.1
- ☑ Windows 10
- ☑ Windows 2003
- ☑ Windows 2008
- ☑ Windows Server 2012
- ☑ Windows Server 2012 R2
- ☑ Windows Server 2016
- ☑ Windows Server 2019
- ☑ Windows Embedded

○ Specify the version of Windows manually:

6. On the **Settings** tab, select **New**.



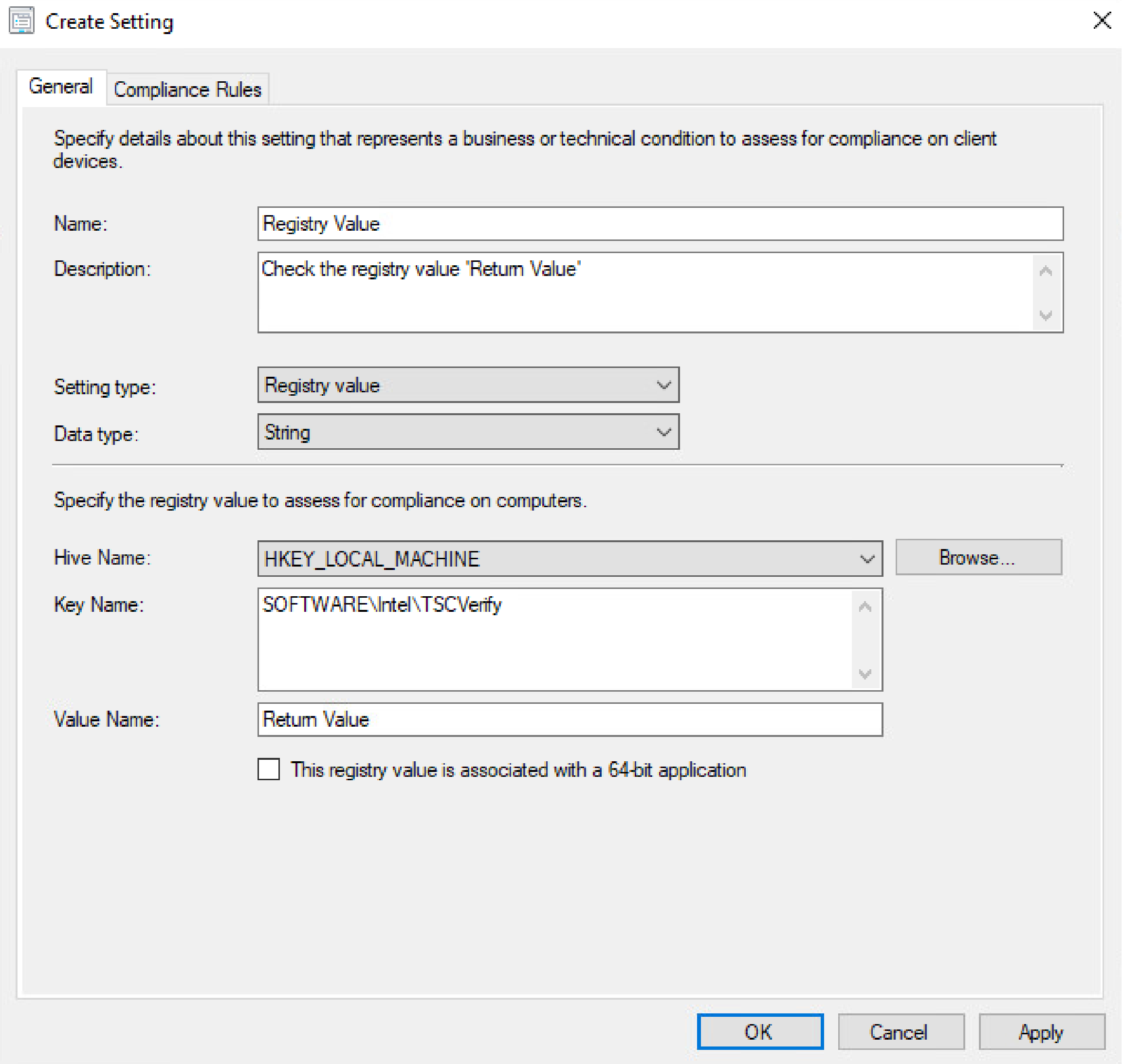
Specify settings for this operating system

Use settings to represent business or technical conditions to assess for compliance on client devices. The following settings are associated with this configuration item.

Name	Setting Type	Inherited	User Setting

There are no items to show in this view.

7. On the **General** tab, enter a name and description in the **Name** and **Description** fields. For **Setting type**, select **Registry value** from the dropdown. For **Data type**, selection **String** from the dropdown. To specify the registry value, select the appropriate **Hive Name** and enter the **Key Name** and **Value Name** in their respective fields. Next, switch to the **Compliance Rules** tab.



Create Setting

Specify details about this setting that represents a business or technical condition to assess for compliance on client devices.

Name: Registry Value

Description: Check the registry value 'Return Value'

Setting type: Registry value

Data type: String

Specify the registry value to assess for compliance on computers.

Hive Name: HKEY_LOCAL_MACHINE

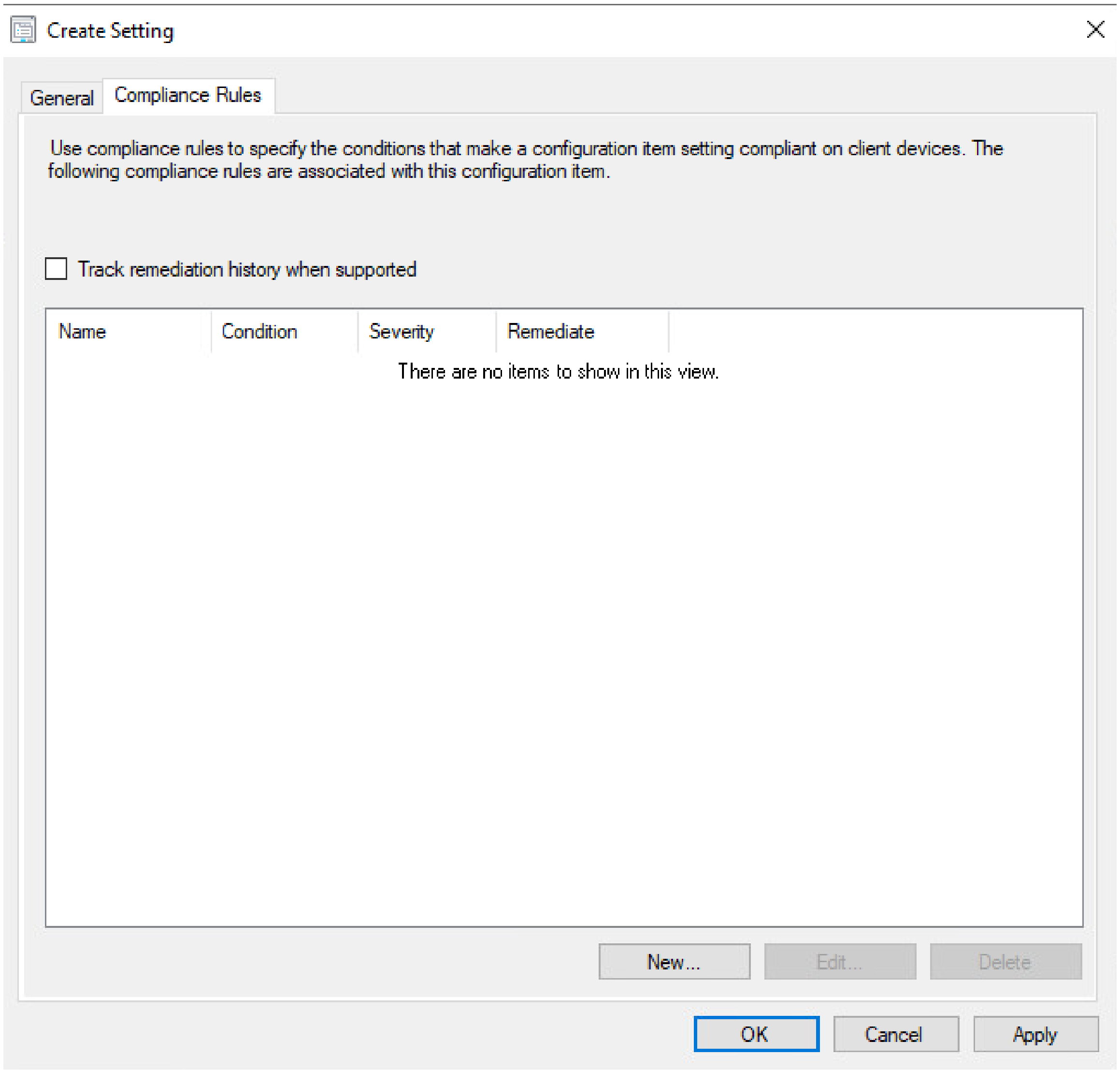
Key Name: SOFTWARE\Intel\TSCVerify

Value Name: Return Value

☐ This registry value is associated with a 64-bit application

739

740 8. Select **New.**



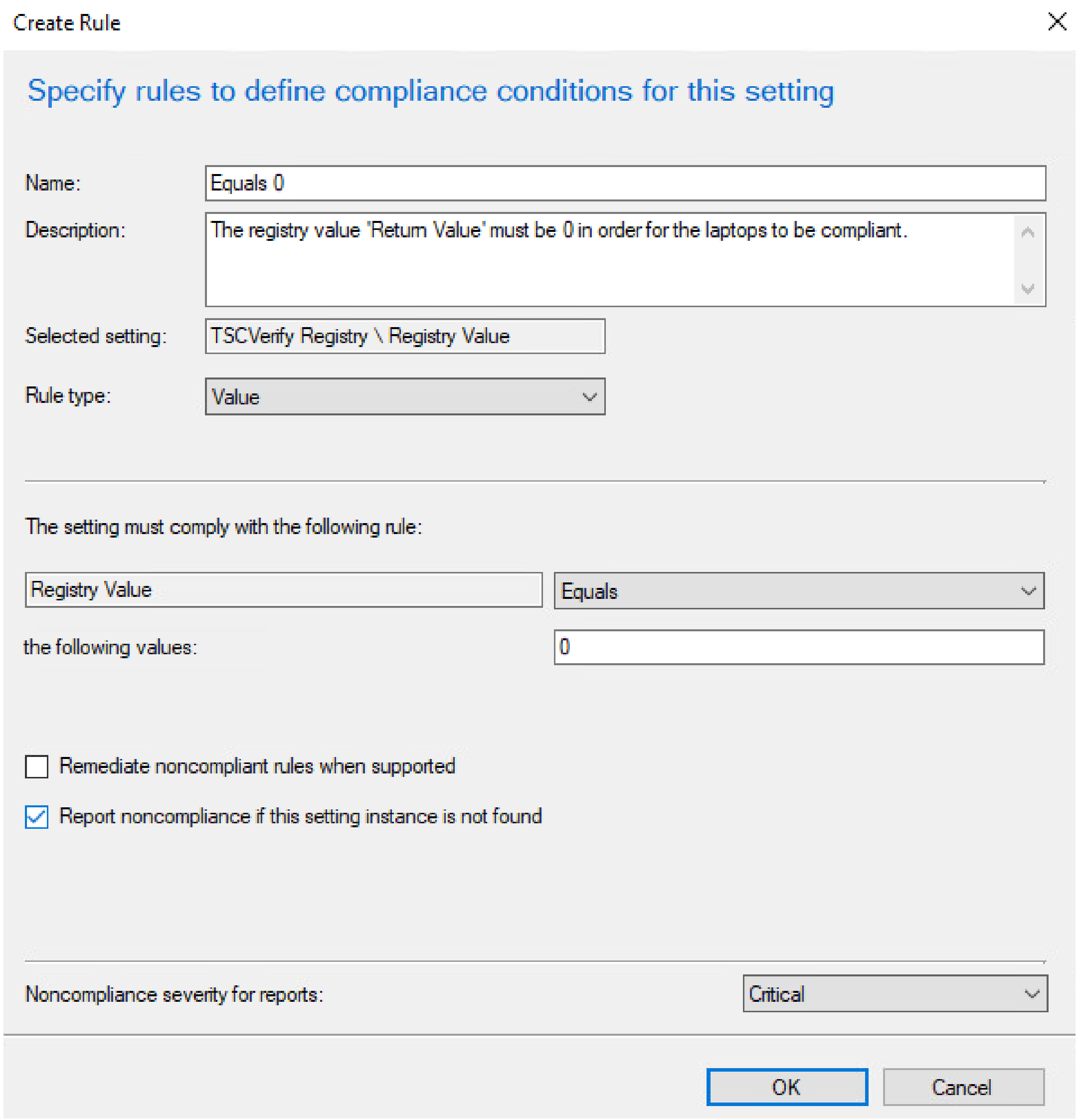
Use compliance rules to specify the conditions that make a configuration item setting compliant on client devices. The following compliance rules are associated with this configuration item.

☐ Track remediation history when supported

Name	Condition	Severity	Remediate

There are no items to show in this view.

9. Specify the name and description for the rule in the **Name** and **Description** fields. For **Rule type**, select **Value** from the dropdown. Under **The setting must comply with the following rule**, select **Registry Value** and **Equals**, and enter 0 (zero) in **the following values:** field. Ensure that **Report noncompliance if this setting instance is not found** is selected. Choose the **Noncompliance severity for reports**. Then select **OK**.



Create Rule

Specify rules to define compliance conditions for this setting

Name: Equals 0

Description: The registry value 'Return Value' must be 0 in order for the laptops to be compliant.

Selected setting: TSCVerify Registry \ Registry Value

Rule type: Value

The setting must comply with the following rule:

Registry Value Equals

the following values: 0

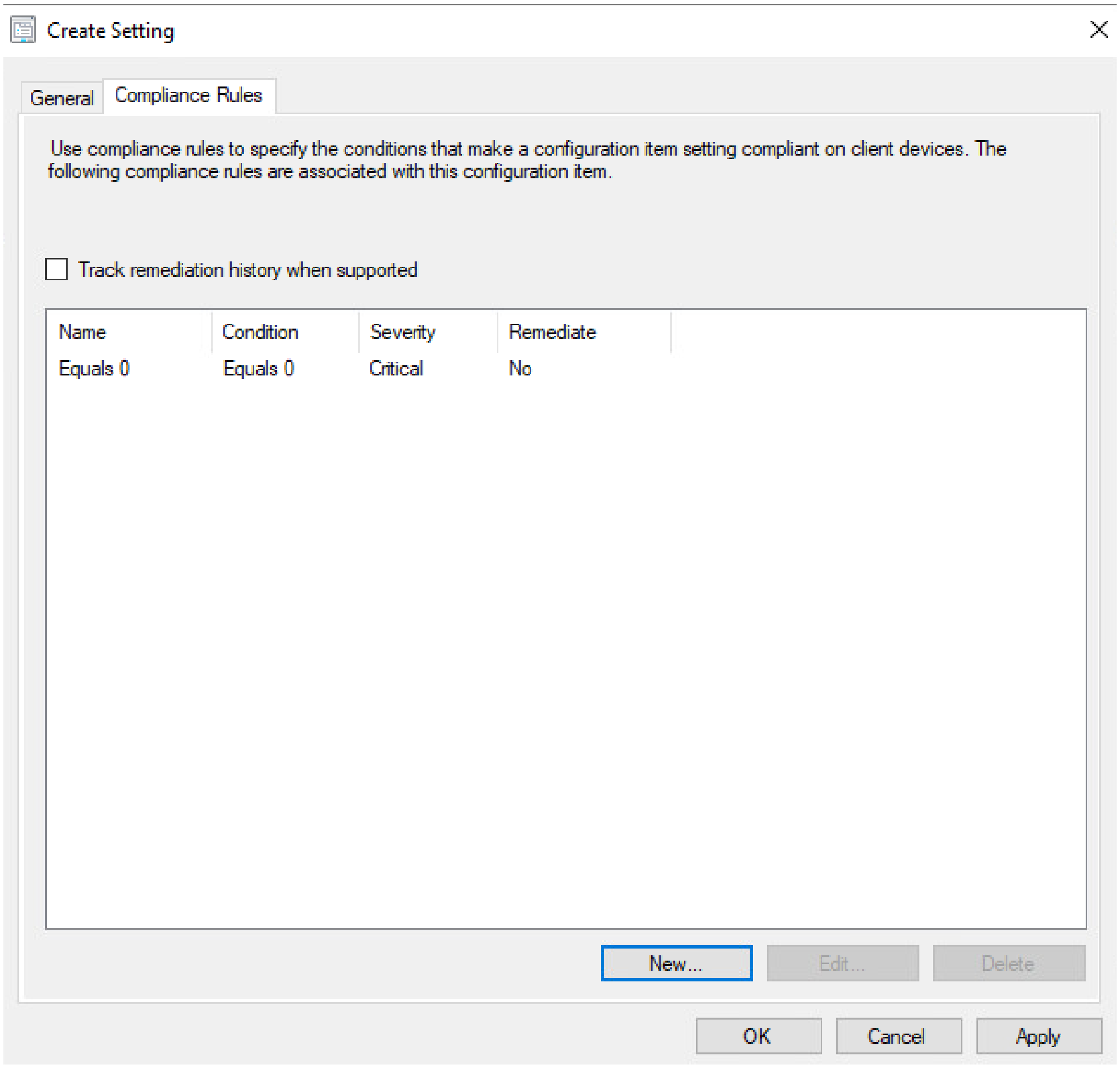
□ Remediate noncompliant rules when supported

☑ Report noncompliance if this setting instance is not found

Noncompliance severity for reports: Critical

747

748 10. Select **Apply**. Then select **OK**.



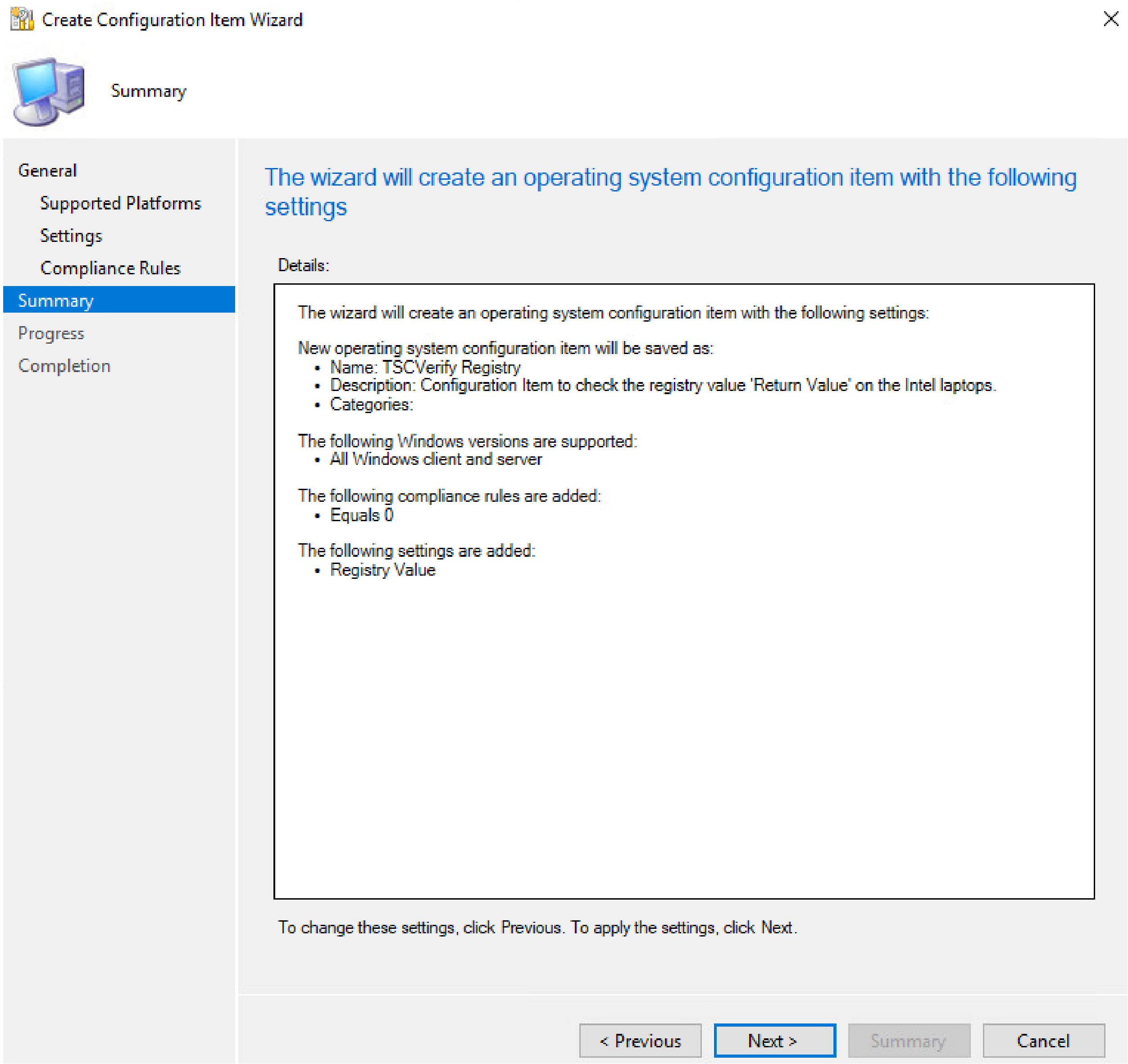
Create Setting

Use compliance rules to specify the conditions that make a configuration item setting compliant on client devices. The following compliance rules are associated with this configuration item.

☐ Track remediation history when supported

Name	Condition	Severity	Remediate
Equals 0	Equals 0	Critical	No

11. Review the configurations on the Summary page. After confirming that the configurations are correct, select **Next**.



The wizard will create an operating system configuration item with the following settings

Details:

The wizard will create an operating system configuration item with the following settings:

New operating system configuration item will be saved as:
- Name: TSCVerify Registry
- Description: Configuration Item to check the registry value 'Return Value' on the Intel laptops.
- Categories:

The following Windows versions are supported:
- All Windows client and server

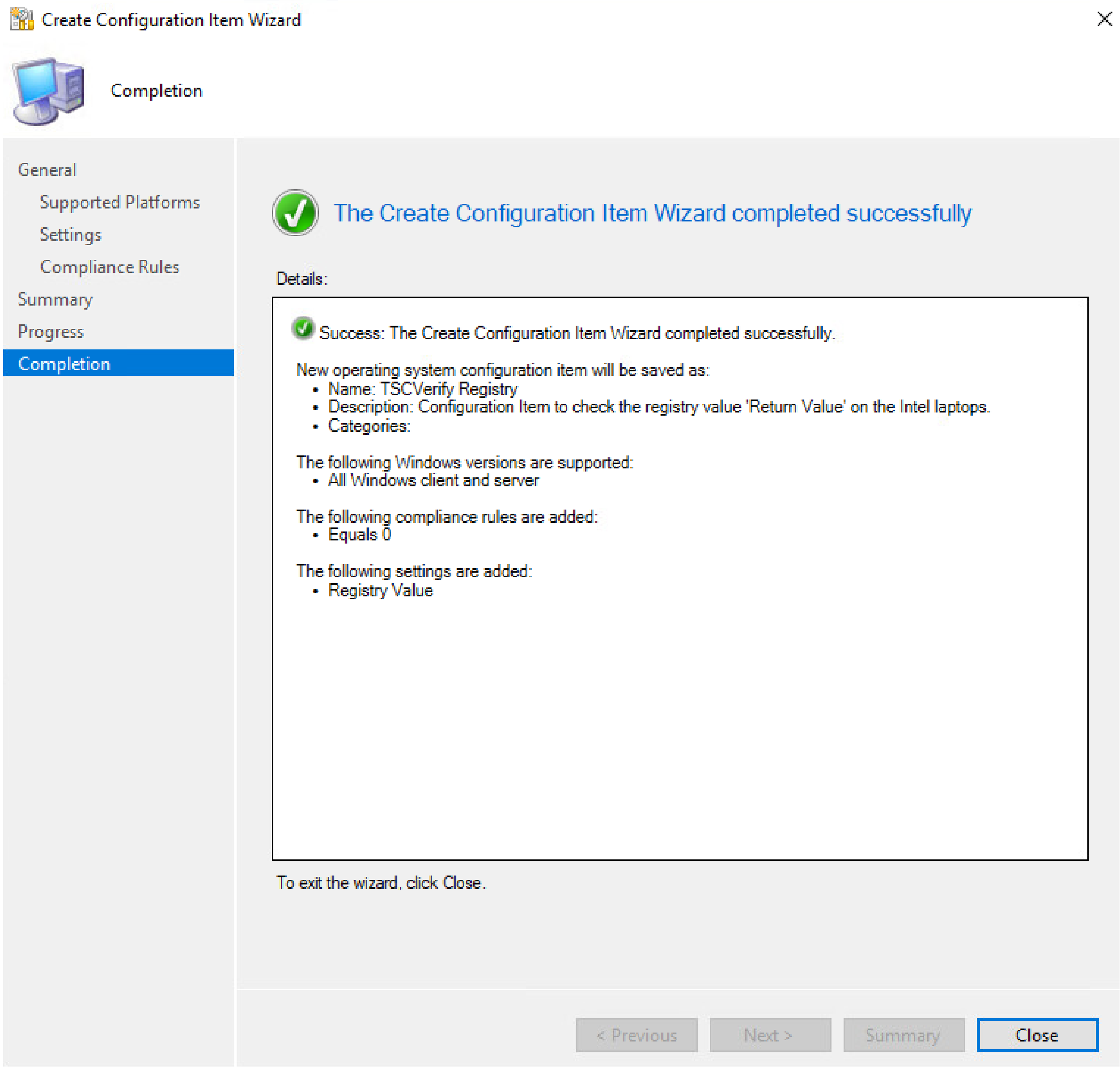
The following compliance rules are added:
- Equals 0

The following settings are added:
- Registry Value

To change these settings, click Previous. To apply the settings, click Next.

752

753 12. After the wizard completes, select **Close.**



The Create Configuration Item Wizard completed successfully

Details:

Success: The Create Configuration Item Wizard completed successfully.

New operating system configuration item will be saved as:

- Name: TSCVerify Registry
- Description: Configuration Item to check the registry value 'Return Value' on the Intel laptops.
- Categories:

The following Windows versions are supported:

- All Windows client and server

The following compliance rules are added:

- Equals 0

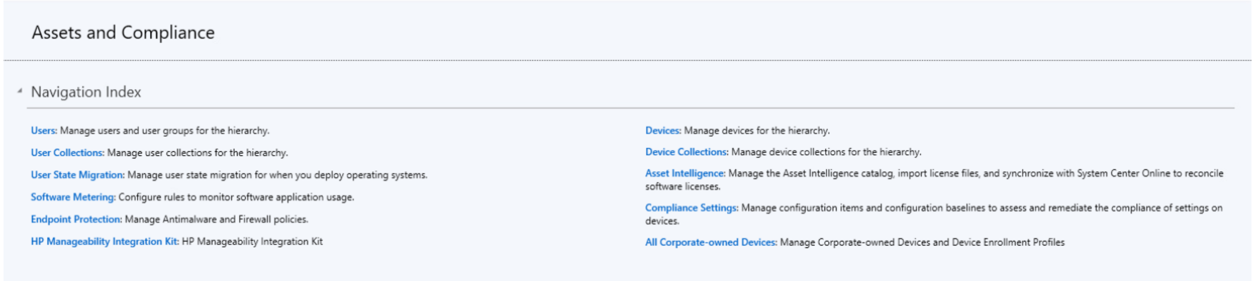
The following settings are added:

- Registry Value

To exit the wizard, click Close.

2.10.1.2 Set Up Configuration Baseline

1. In the Microsoft Endpoint Configuration Manager console, under **Assets and Compliance > Overview**, select **Compliance Settings**.



Assets and Compliance

Navigation Index

Users: Manage users and user groups for the hierarchy.

User Collections: Manage user collections for the hierarchy.

User State Migration: Manage user state migration for when you deploy operating systems.

Software Metering: Configure rules to monitor software application usage.

Endpoint Protection: Manage Antimalware and Firewall policies.

HP Manageability Integration Kit: HP Manageability Integration Kit

Devices: Manage devices for the hierarchy.

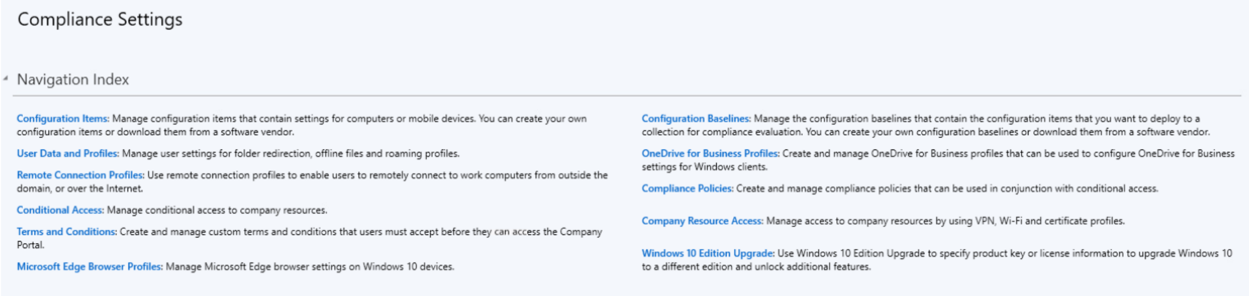
Device Collections: Manage device collections for the hierarchy.

Asset Intelligence: Manage the Asset Intelligence catalog, import license files, and synchronize with System Center Online to reconcile software licenses.

Compliance Settings: Manage configuration items and configuration baselines to assess and remediate the compliance of settings on devices.

All Corporate-owned Devices: Manage Corporate-owned Devices and Device Enrollment Profiles

2. Next, select **Configuration Baselines**.



Compliance Settings

Navigation Index

Configuration Items: Manage configuration items that contain settings for computers or mobile devices. You can create your own configuration items or download them from a software vendor.

User Data and Profiles: Manage user settings for folder redirection, offline files and roaming profiles.

Remote Connection Profiles: Use remote connection profiles to enable users to remotely connect to work computers from outside the domain, or over the Internet.

Conditional Access: Manage conditional access to company resources.

Terms and Conditions: Create and manage custom terms and conditions that users must accept before they can access the Company Portal.

Microsoft Edge Browser Profiles: Manage Microsoft Edge browser settings on Windows 10 devices.

Configuration Baselines: Manage the configuration baselines that contain the configuration items that you want to deploy to a collection for compliance evaluation. You can create your own configuration baselines or download them from a software vendor.

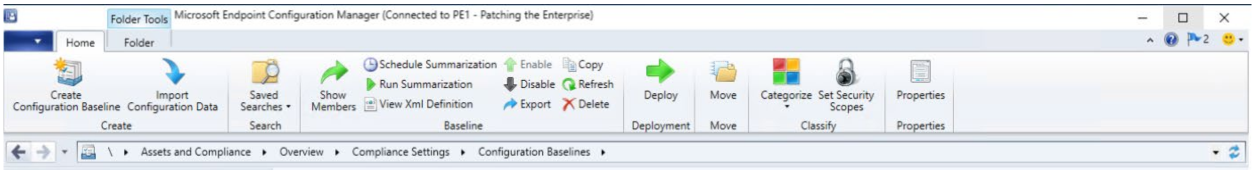
OneDrive for Business Profiles: Create and manage OneDrive for Business profiles that can be used to configure OneDrive for Business settings for Windows clients.

Compliance Policies: Create and manage compliance policies that can be used in conjunction with conditional access.

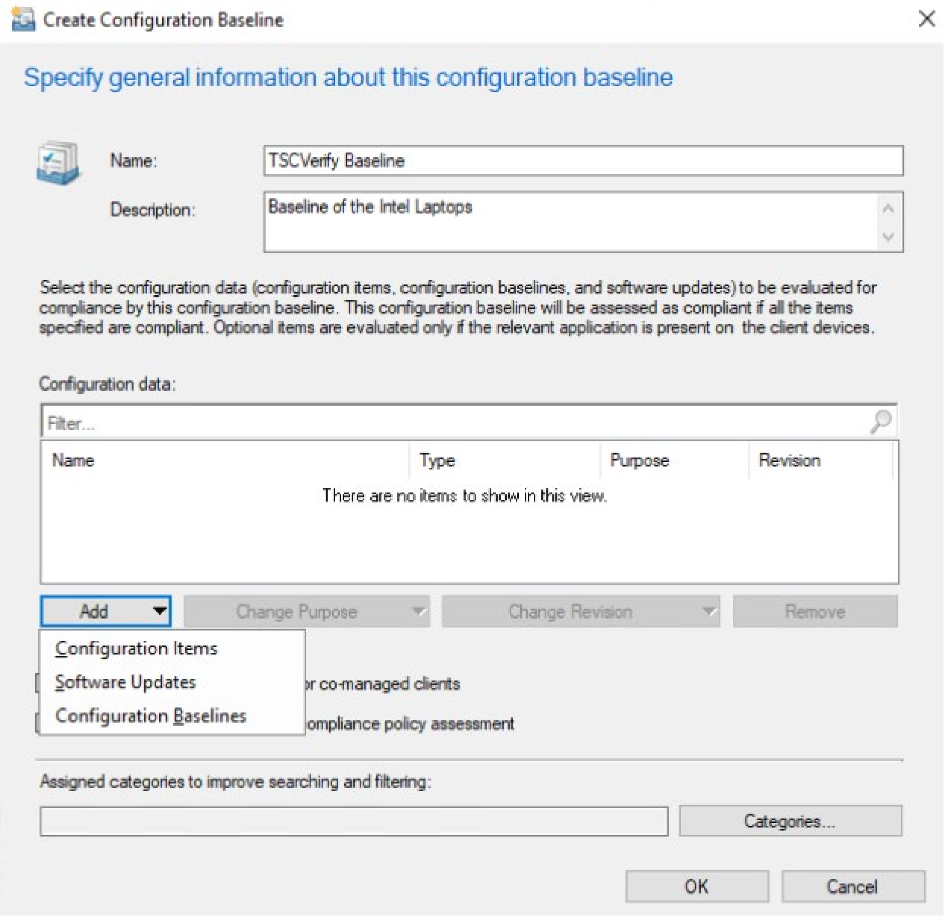
Company Resource Access: Manage access to company resources by using VPN, Wi-Fi and certificate profiles.

Windows 10 Edition Upgrade: Use Windows 10 Edition Upgrade to specify product key or license information to upgrade Windows 10 to a different edition and unlock additional features.

3. From the **Home** panel at the top, select **Create Configuration Baseline**.



4. Provide a name and description for the configuration baseline in the **Name** and **Description** fields. Next, select **Add** and choose **Configuration Items**.



765

Create Configuration Baseline

Specify general information about this configuration baseline

Name: TSCVerify Baseline

Description: Baseline of the Intel Laptops

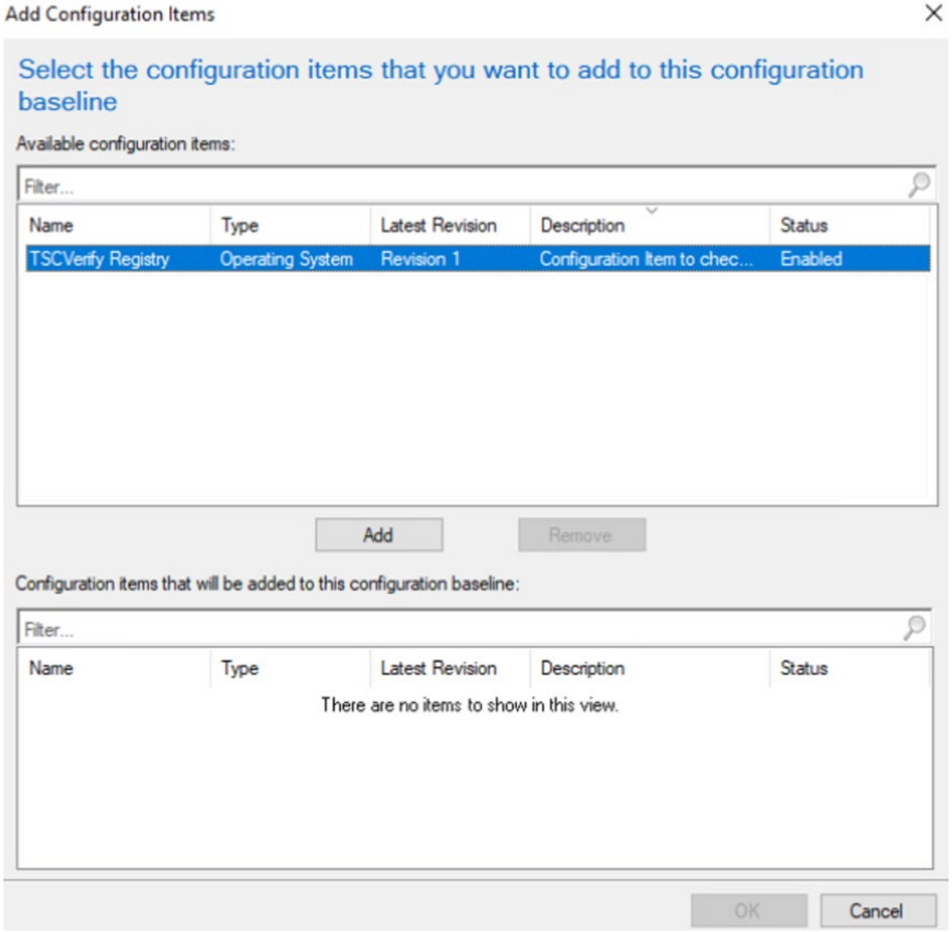
Select the configuration data (configuration items, configuration baselines, and software updates) to be evaluated for compliance by this configuration baseline. This configuration baseline will be assessed as compliant if all the items specified are compliant. Optional items are evaluated only if the relevant application is present on the client devices.

Configuration data:

Name	Type	Purpose	Revision

There are no items to show in this view.

5. Select the previously created configuration item from the list and select **Add**.



Add Configuration Items

Select the configuration items that you want to add to this configuration baseline

Available configuration items:

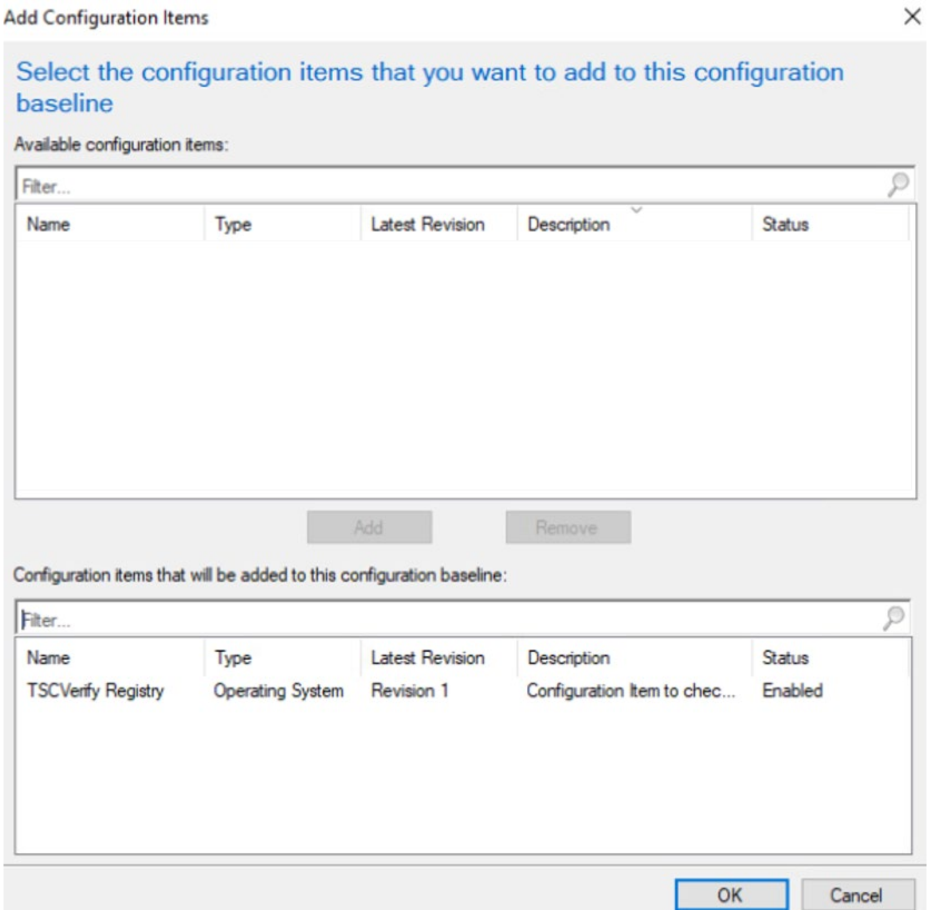
Name	Type	Latest Revision	Description	Status
TSCVerify Registry	Operating System	Revision 1	Configuration Item to chec...	Enabled

Configuration items that will be added to this configuration baseline:

Name	Type	Latest Revision	Description	Status

There are no items to show in this view.

6. Select **OK**.

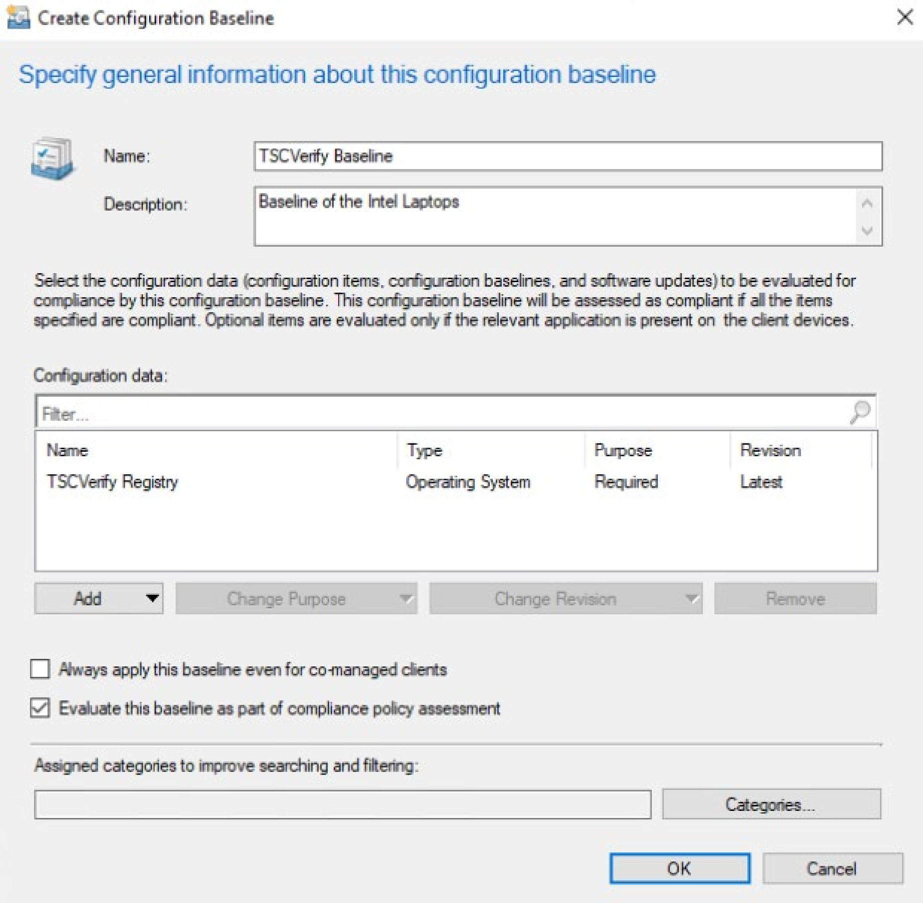


Add Configuration Items
Select the configuration items that you want to add to this configuration baseline
Available configuration items:
Filter...
Add
Remove
Configuration items that will be added to this configuration baseline:
Filter...
OK
Cancel

Name	Type	Latest Revision	Description	Status
TSCVerify Registry	Operating System	Revision 1	Configuration Item to chec...	Enabled

769

770 7. Select **OK**.



Create Configuration Baseline

Specify general information about this configuration baseline

Name: TSCVerify Baseline

Description: Baseline of the Intel Laptops

Select the configuration data (configuration items, configuration baselines, and software updates) to be evaluated for compliance by this configuration baseline. This configuration baseline will be assessed as compliant if all the items specified are compliant. Optional items are evaluated only if the relevant application is present on the client devices.

Configuration data:

Name	Type	Purpose	Revision
TSCVerify Registry	Operating System	Required	Latest

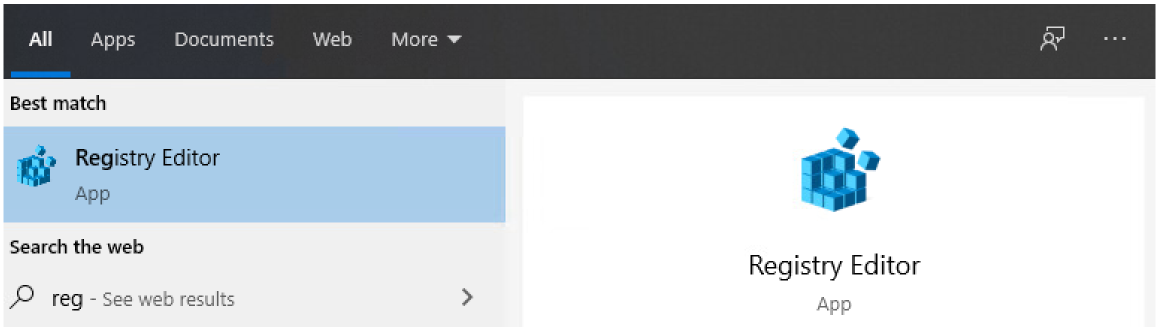
☐ Always apply this baseline even for co-managed clients

☑ Evaluate this baseline as part of compliance policy assessment

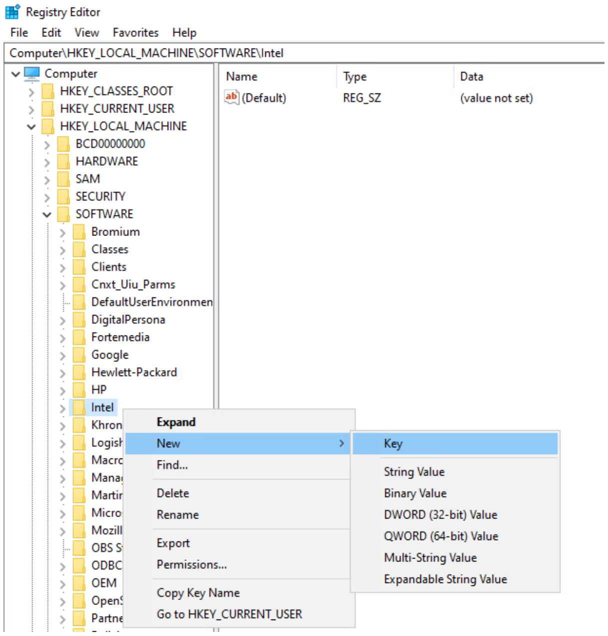
Assigned categories to improve searching and filtering:

2.10.1.3 Set Up Registry Entry on Intel Devices

1. On the Windows 10 laptop, go to **Start**, search for the **Registry Editor,** and open that program.

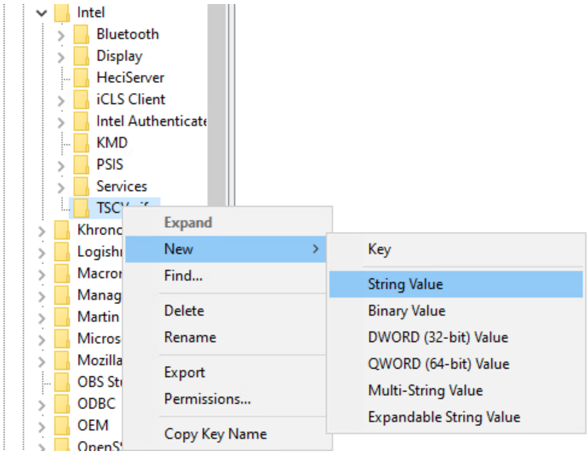


2. Find the Intel folder located in **HKEY_LOCAL_MACHINE\SOFTWARE**. Right click and select **New > Key**. Name the key **TSCVerify**.

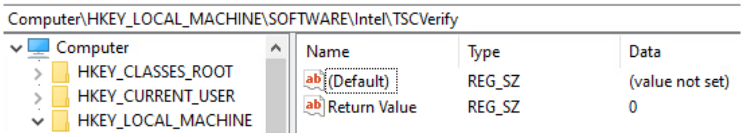


Name	Type	Data
(Default)	REG_SZ	(value not set)

3. Select the **TSCVerify** key, right-click and select **New > String Value**.



4. Enter *Return Value* in the **Name** field.



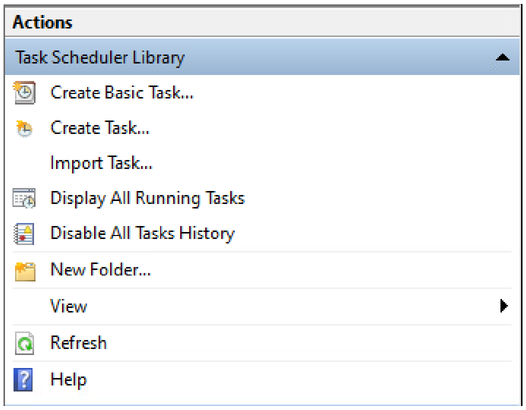
Name	Type	Data
(Default)	REG_SZ	(value not set)
Return Value	REG_SZ	0

2.10.1.4Run Script Via Task Manager

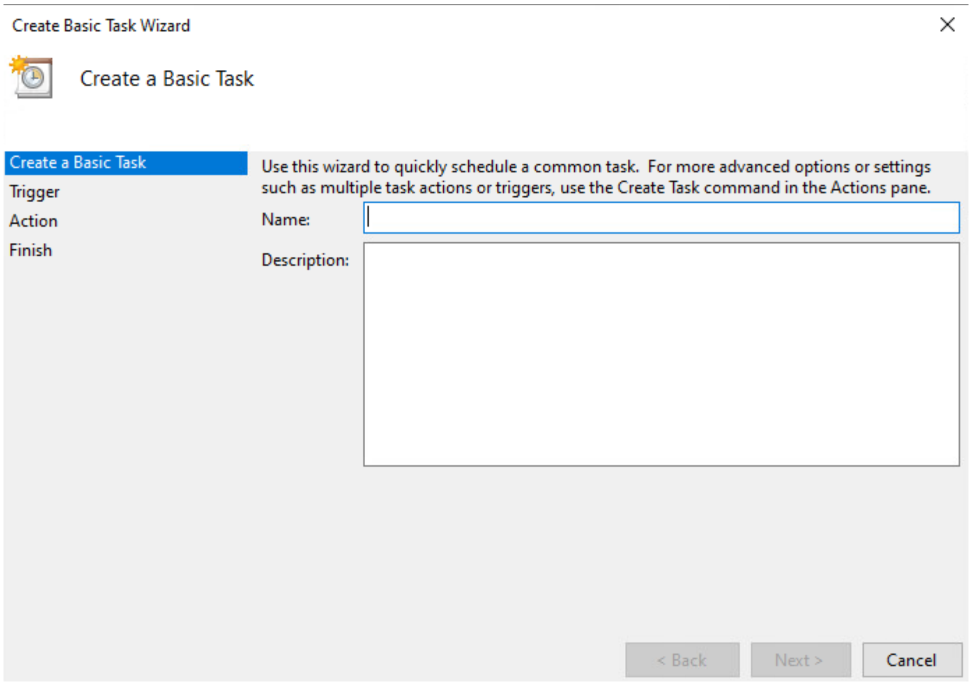
1. Place the script onto the local machine (snippet shown below). A copy of this script can be obtained from our repository.

```
    # Run Scan and capture exit code.
    # 0=No components have changed and platform certificate validation passed
    # 1=At least one component has changed OR platform certificate validation
failed
    # 2=At least one component has changed AND Platform Certificate validation
failed

    # Write-Output "Starting DPD file scan and compare..."
    $tscpinfo = New-Object System.Diagnostics.ProcessStartInfo
    $tscpinfo.FileName = "TSCVerifyTool_3.40.exe"
    $tscpinfo.WorkingDirectory = $artifactdirectory
    $tscpinfo.RedirectStandardError = $true
    $tscpinfo.RedirectStandardOutput = $true
    $tscpinfo.UseShellExecute = $false
    $tscpinfo.Arguments = "SCANREADCOMP -in $dpdfile"
    $dpdprocess = New-Object System.Diagnostics.Process
    $dpdprocess.StartInfo = $tscpinfo
    $dpdprocess.Start() | Out-Null
    $stdout = $dpdprocess.StandardOutput.ReadToEnd()
    $dpdprocess.WaitForExit()

    # Write-Output "Starting Platform Certificate validation ..."
    $tscpinfo.Arguments = "PFORMCRTCOMP -in $platformcertificatefile"
    $platformcertprocess = New-Object System.Diagnostics.Process
    $platformcertprocess.StartInfo = $tscpinfo
    $platformcertprocess.Start() | Out-Null
    $stdout = $platformcertprocess.StandardOutput.ReadToEnd()
    $platformcertprocess.WaitForExit()

    # If the return value is nonzero, then the computer is not compliant
    $retValue = $dpdprocess.ExitCode + $platformcertprocess.ExitCode
    Write-Output $retValue

    # Add retValue to registry location
    $regPath = "HKLM:\SOFTWARE\Intel\TSCVerify"
    Set-ItemProperty -Path $regPath -Name "Return Value" -Value $retValue
```

2. From the **Start Menu**, search for **Task Scheduler** and open the program.
3. Under the **Actions** panel, select **Create Basic Task**.



4. Fill in the **Name** and **Description** fields. Then select **Next**.

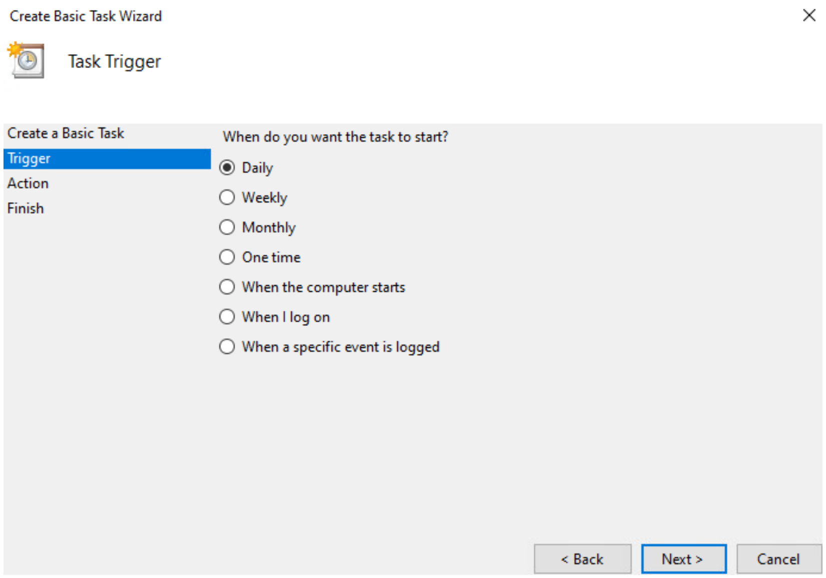


Use this wizard to quickly schedule a common task. For more advanced options or settings such as multiple task actions or triggers, use the Create Task command in the Actions pane.

Name:

Description:

5. Select the frequency for this task to run. Then select **Next**.



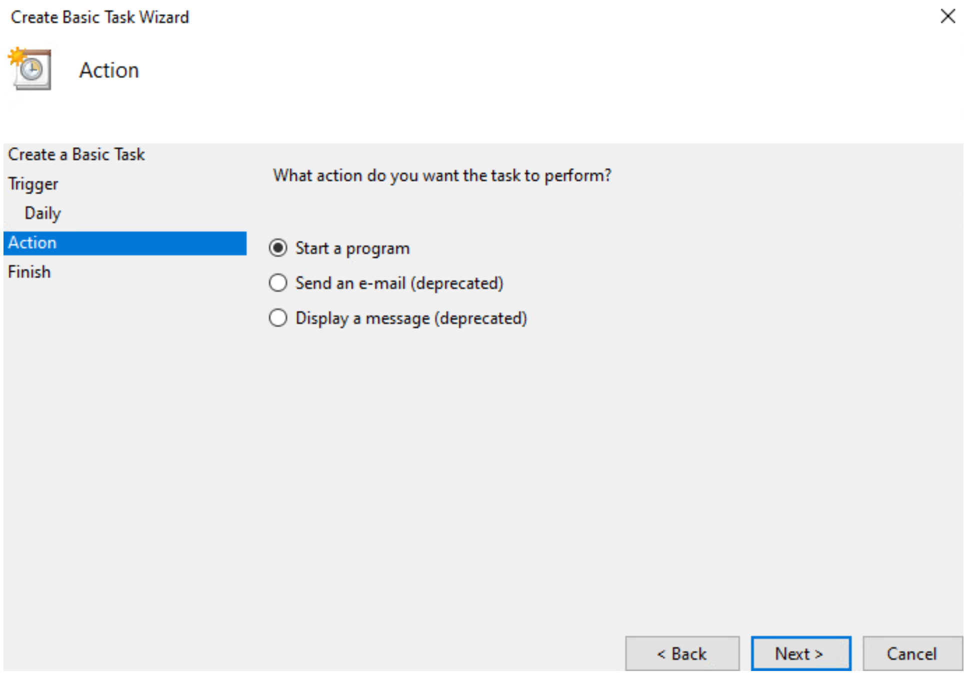
Create Basic Task Wizard

Task Trigger

When do you want the task to start?

- ● Daily
- ○ Weekly
- ○ Monthly
- ○ One time
- ○ When the computer starts
- ○ When I log on
- ○ When a specific event is logged

6. Select the start date and time for the task. Then select **Next**.
7. Select the action **Start a program**. Then select **Next**.



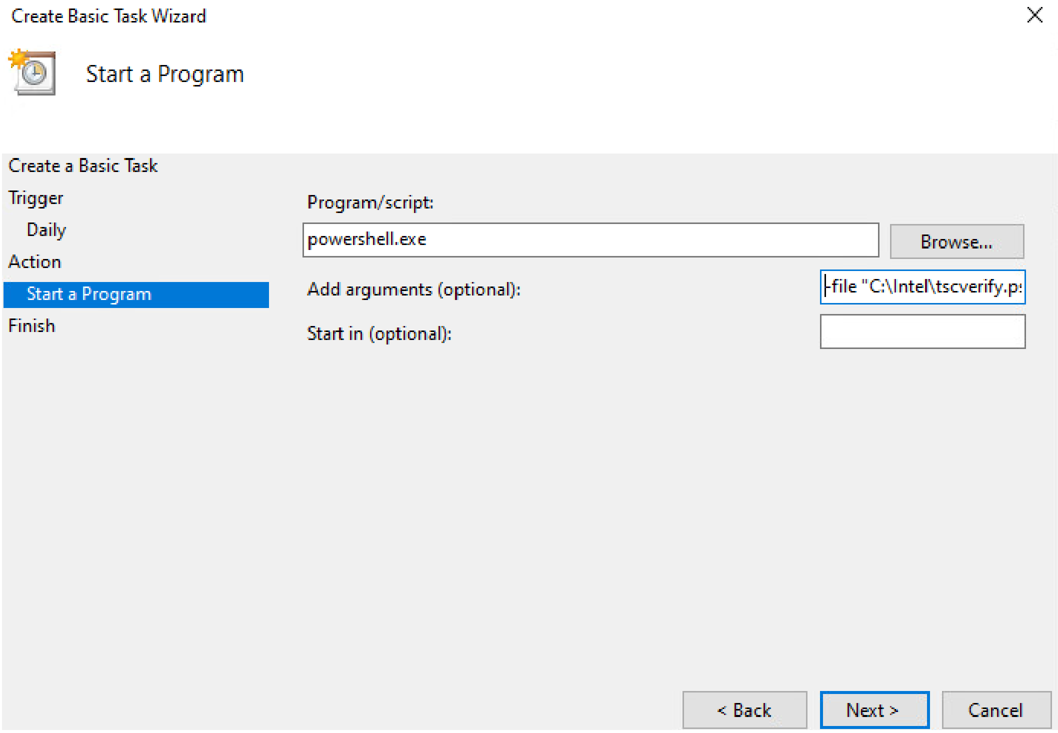
Create Basic Task Wizard

Action

What action do you want the task to perform?

- ● Start a program
- ○ Send an e-mail (deprecated)
- ○ Display a message (deprecated)

8. In the **Start a program** section, type the following in the **Program/script** field: *powershell.exe*. Next, add the following to the add arguments (optional) field: *-file “<Location of script>”*. Then select **Next**.

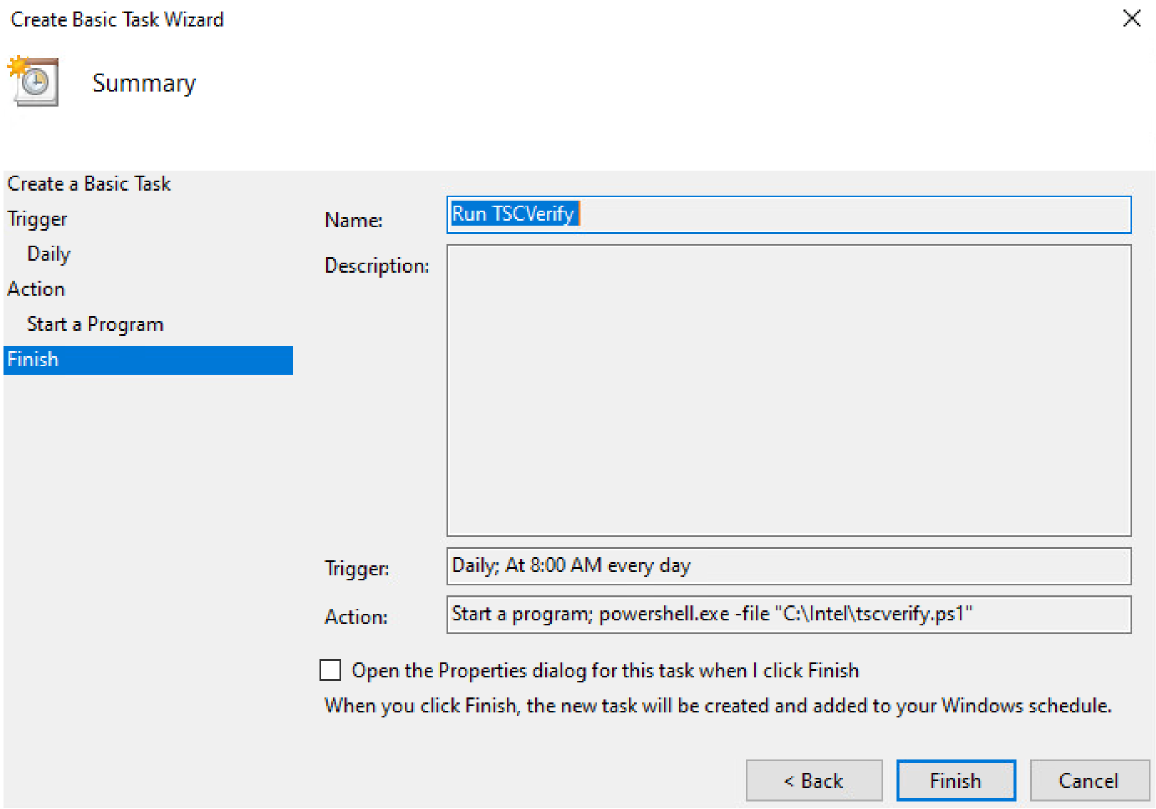


Program/script: powershell.exe

Add arguments (optional): -file "C:\Intel\tscverify.p

Start in (optional):

9. Confirm the settings are correct and select **Finish**.



Name: Run TSCVerify

Description:

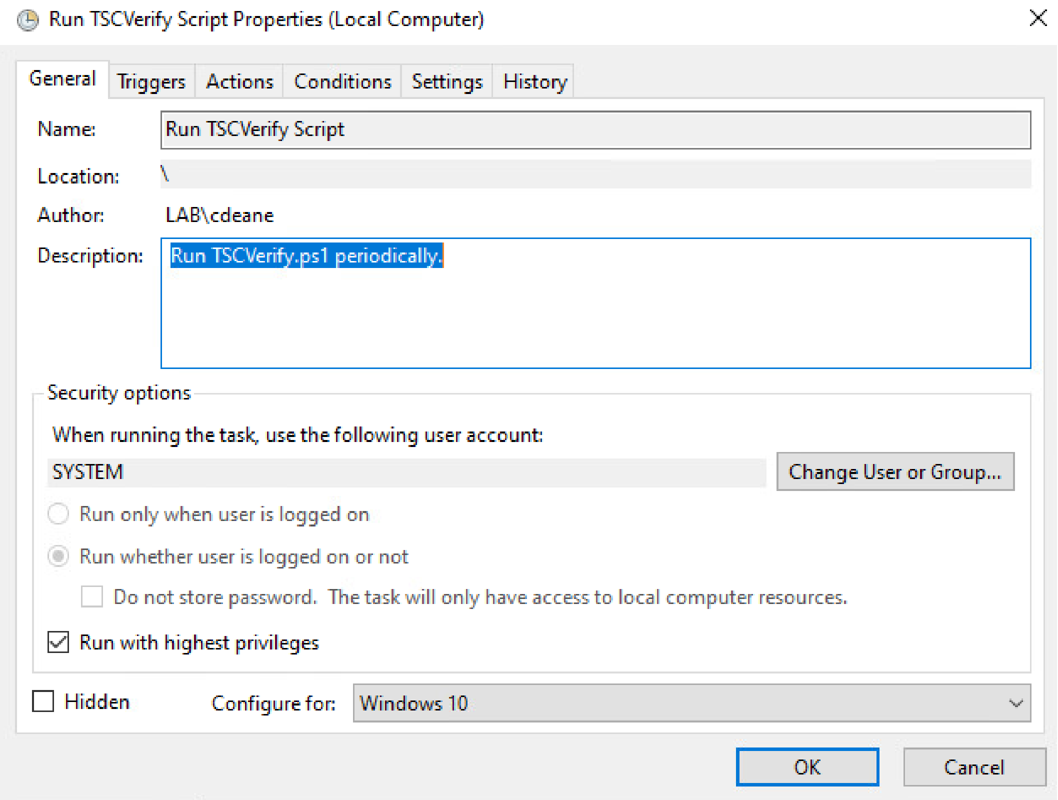
Trigger: Daily; At 8:00 AM every day

Action: Start a program; powershell.exe -file "C:\Intel\tscverify.ps1"

☐ Open the Properties dialog for this task when I click Finish

When you click Finish, the new task will be created and added to your Windows schedule.

10. On the main page of Task Scheduler, select the newly created task, right-click it, and select **Properties**.
11. On the **General** tab, under **Security Options**, change the user to **SYSTEM**. Next, ensure that the option **Run with highest privileges** is checked.



Run TSCVerify Script Properties (Local Computer)

Name: Run TSCVerify Script

Location: \

Author: LAB\cdeane

Description: Run TSCVerify.ps1 periodically.

Security options

When running the task, use the following user account:

SYSTEM

○ Run only when user is logged on

● Run whether user is logged on or not

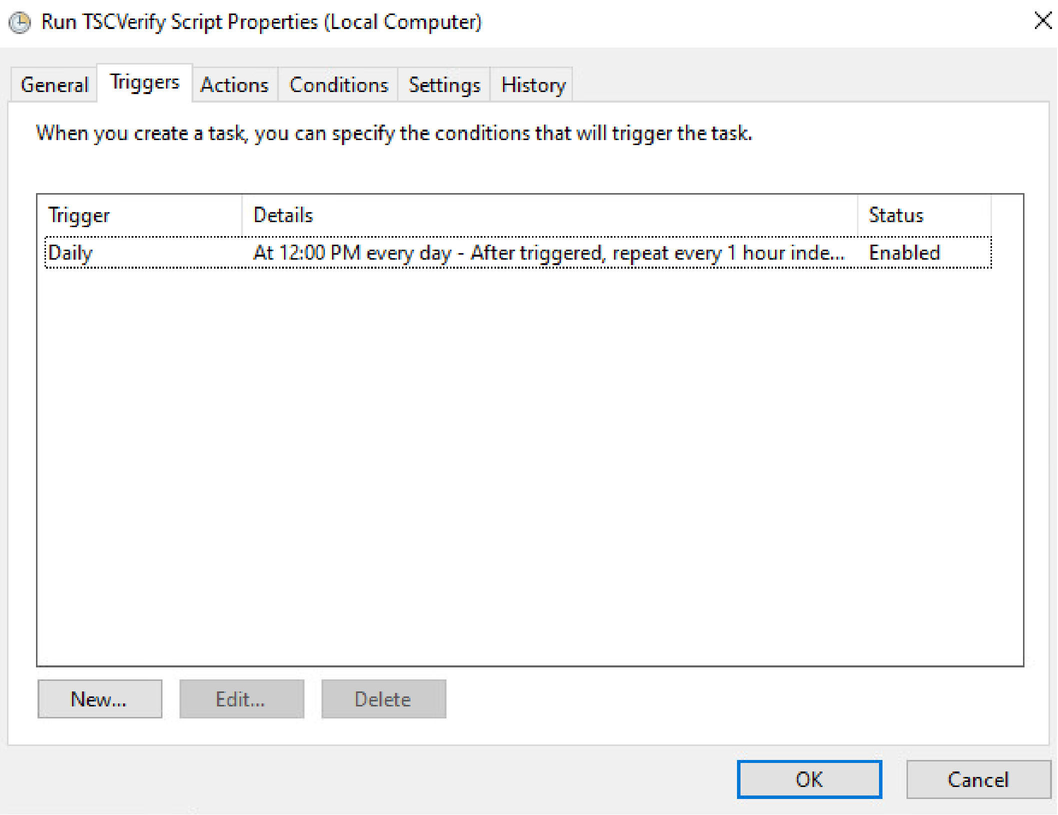
□ Do not store password. The task will only have access to local computer resources.

☑ Run with highest privileges

□ Hidden

Configure for: Windows 10

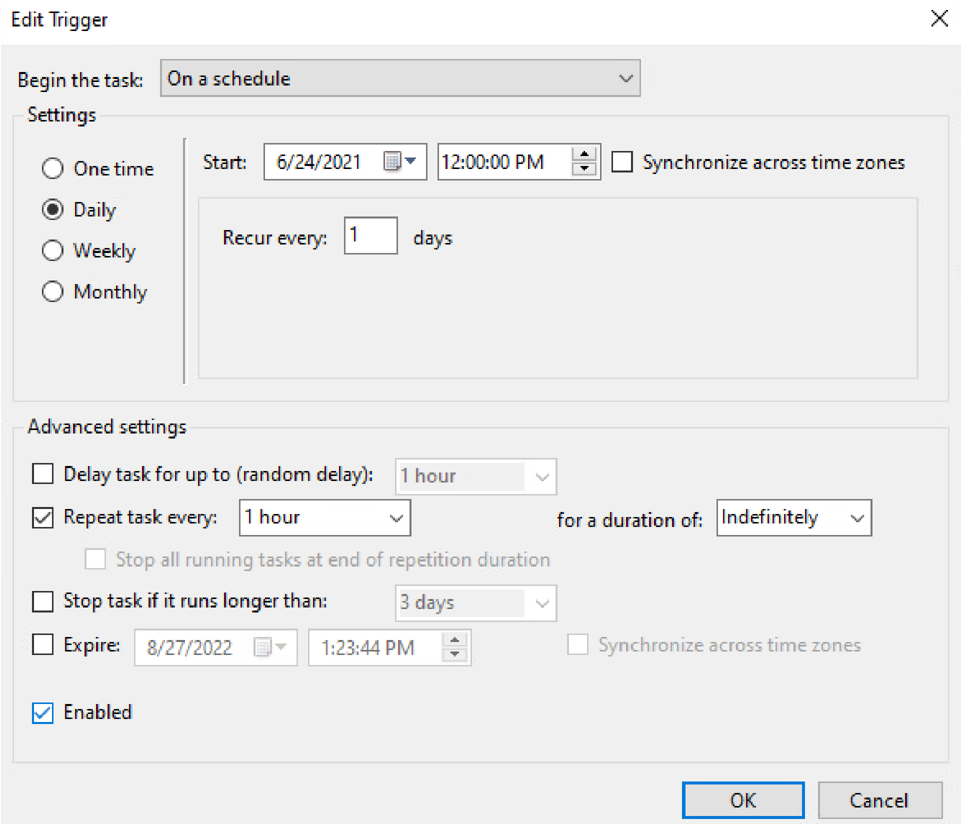
12. Navigate to the **Triggers** tab. Select the existing trigger and select **Edit**.



When you create a task, you can specify the conditions that will trigger the task.

Trigger	Details	Status
Daily	At 12:00 PM every day - After triggered, repeat every 1 hour inde...	Enabled

13. Under the **Advanced Settings** section, ensure that **Repeat task every 1 hour for a duration of Indefinitely** is checked, as well as **Enabled**. Select **OK**.



Edit Trigger

Begin the task: On a schedule

Settings

○ One time
● Daily
○ Weekly
○ Monthly

Start: 6/24/2021 12:00:00 PM □ Synchronize across time zones

Recur every: 1 days

Advanced settings

□ Delay task for up to (random delay): 1 hour

☑ Repeat task every: 1 hour for a duration of: Indefinitely

□ Stop all running tasks at end of repetition duration

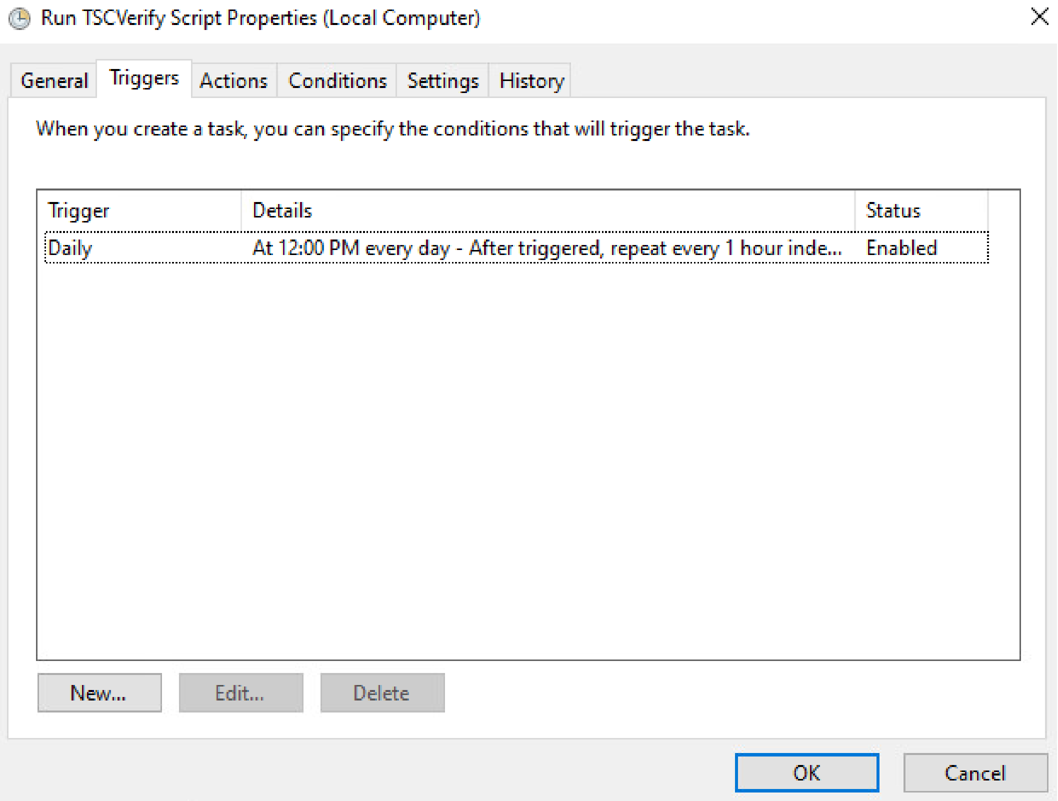
□ Stop task if it runs longer than: 3 days

□ Expire: 8/27/2022 1:23:44 PM □ Synchronize across time zones

☑ Enabled

846

847 14. Select **OK**.

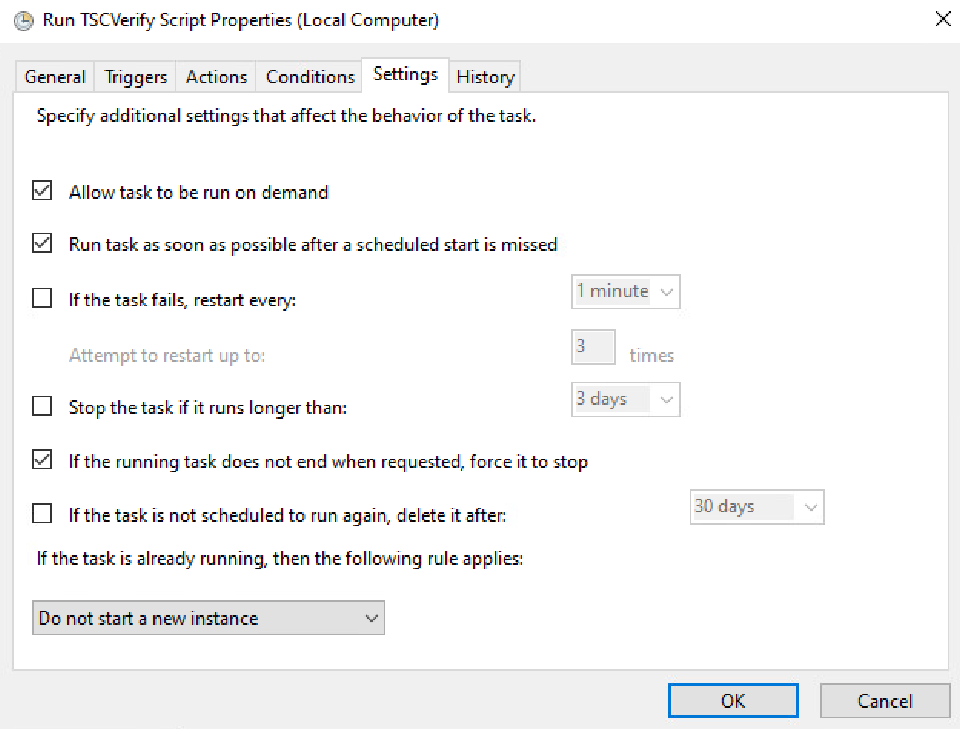


Run TSCVerify Script Properties (Local Computer)

When you create a task, you can specify the conditions that will trigger the task.

Trigger	Details	Status
Daily	At 12:00 PM every day - After triggered, repeat every 1 hour inde...	Enabled

15. Navigate to the **Settings** Tab and ensure the following are checked, then select **OK**:
    - Allow task to be run on demand
    - Run task as soon as possible after a scheduled start is missed
    - If the running task does not end when requested, force it to stop



Specify additional settings that affect the behavior of the task.

☑ Allow task to be run on demand

☑ Run task as soon as possible after a scheduled start is missed

☐ If the task fails, restart every: 1 minute

Attempt to restart up to: 3 times

☐ Stop the task if it runs longer than: 3 days

☑ If the running task does not end when requested, force it to stop

☐ If the task is not scheduled to run again, delete it after: 30 days

If the task is already running, then the following rule applies:

Do not start a new instance

2.10.2 RSA Archer DataFeed Integrations

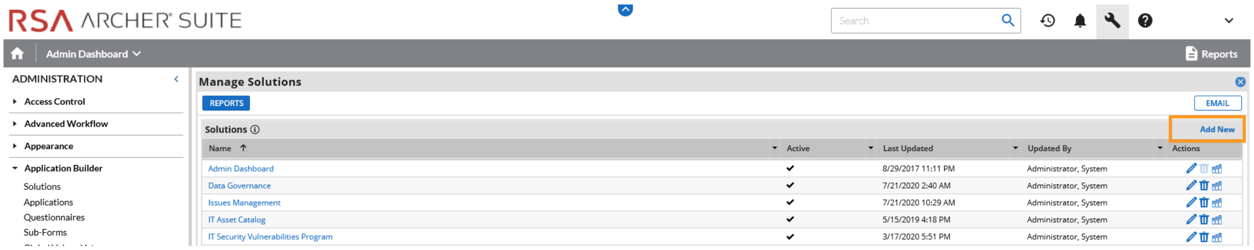
RSA Archer serves a dual role in the prototype demonstration - the Asset Management and Discovery System and the IT Administrator Dashboard. This section will detail the steps necessary to integrate RSA Archer with the PMCS, the Eclypsium Firmware Analytics Platform, and Microsoft Configuration Manager, which will form the basis of the Asset Management and Discovery System. From there, we will describe how to create a dashboard using the data gathered from the preceding integrations.

2.10.2.1 Create the Devices Application

Before platform and firmware data can be stored in the in the Asset Management and Discovery System, the RSA Archer application must be created. For this task, we leverage the default *Devices* application described as *the central repository of knowledge about your business-critical devices…*

We use the Devices application as a starting point for our customizations that are described in the section. Your organization may have additional requirements that can also be integrated into this solution. As a user with administrative privileges, ensure your installation has the *IT Asset Catalog* solution included before starting the following procedures.

1. In the administration menu, navigate to **Application Builder** -> **Solutions**. Select **Add New**.

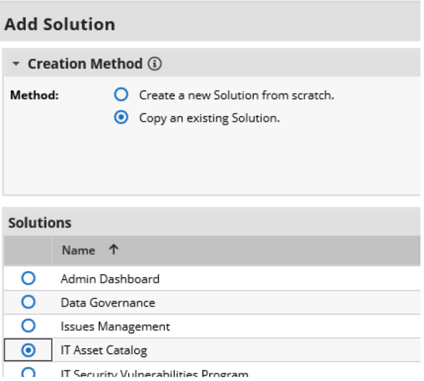


Manage Solutions

Solutions

Name	Active	Last Updated	Updated By	Actions
Admin Dashboard	✓	8/29/2017 11:11 PM	Administrator, System	
Data Governance	✓	7/21/2020 2:40 AM	Administrator, System	
Issues Management	✓	7/21/2020 10:29 AM	Administrator, System	
IT Asset Catalog	✓	5/15/2019 4:18 PM	Administrator, System	
IT Security Vulnerabilities Program	✓	3/17/2020 5:51 PM	Administrator, System	

2. Select **Copy an existing Solution** and the **IT Asset Catalog**. Click **OK**.



Add Solution

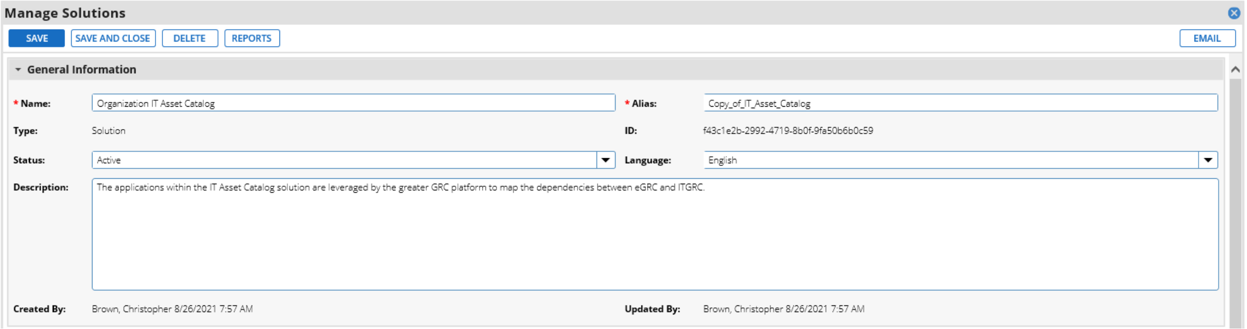
Creation Method

Method: ○ Create a new Solution from scratch.
● Copy an existing Solution.

Solutions

	Name
○	Admin Dashboard
○	Data Governance
○	Issues Management
●	IT Asset Catalog
○	IT Security Vulnerabilities Program

3. Enter an identifier for the catalog in the **Name** field. Click **SAVE AND CLOSE**.



Manage Solutions

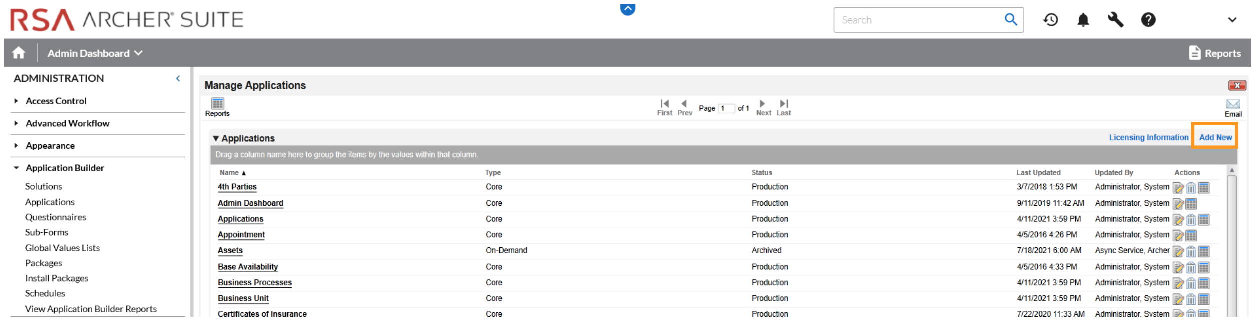
General Information

* Name:	Organization IT Asset Catalog	* Alias:	Copy_of_IT_Asset_Catalog
Type:	Solution	ID:	f43c1e2b-2992-4719-8b0f-9fa50b6b0c59
Status:	Active	Language:	English
Description:	The applications within the IT Asset Catalog solution are leveraged by the greater GRC platform to map the dependencies between eGRC and ITGRC.		
Created By:	Brown, Christopher 8/26/2021 7:57 AM	Updated By:	Brown, Christopher 8/26/2021 7:57 AM

2.10.2.1.1 Create Supporting Applications

Next, create custom applications that will augment the default *Devices* application. The first application will store the components associated with each computing device that satisfies acceptance testing.

1. In the administration menu, navigate to **Application Builder -> Applications**. Select ***Add New***.



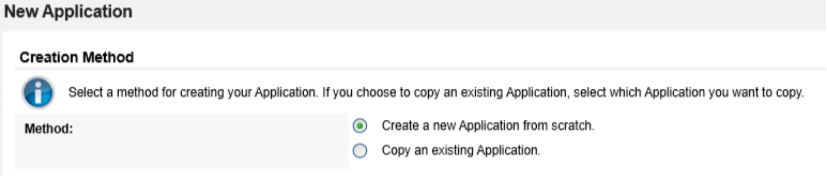
Manage Applications

Applications

Drag a column name here to group the items by the values within that column.

Name ▲	Type	Status	Last Updated	Updated By	Actions
4th Parties	Core	Production	3/7/2018 1:53 PM	Administrator, System	
Admin Dashboard	Core	Production	9/11/2019 11:42 AM	Administrator, System	
Applications	Core	Production	4/11/2021 3:59 PM	Administrator, System	
Appointment	Core	Production	4/5/2016 4:26 PM	Administrator, System	
Assets	On-Demand	Archived	7/18/2021 6:00 AM	Async Service, Archer	
Base Availability	Core	Production	4/5/2016 4:33 PM	Administrator, System	
Business Processes	Core	Production	4/11/2021 3:59 PM	Administrator, System	
Business Unit	Core	Production	4/11/2021 3:59 PM	Administrator, System	
Certificates of Insurance	Core	Production	7/22/2020 11:33 AM	Administrator, System	

2. Select **Create a new Application from scratch** and click **OK**.



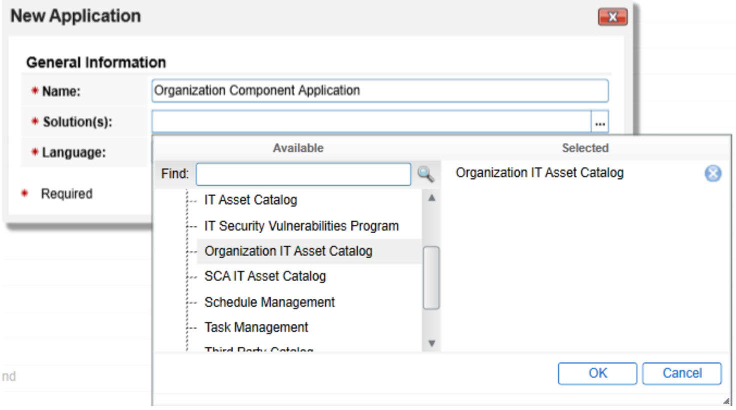
New Application

Creation Method

Select a method for creating your Application. If you choose to copy an existing Application, select which Application you want to copy.

Method:
● Create a new Application from scratch.
○ Copy an existing Application.

3. Create an identifier in the **Name** field and select the solution created earlier. Click **OK**.



New Application

General Information

* Name: Organization Component Application

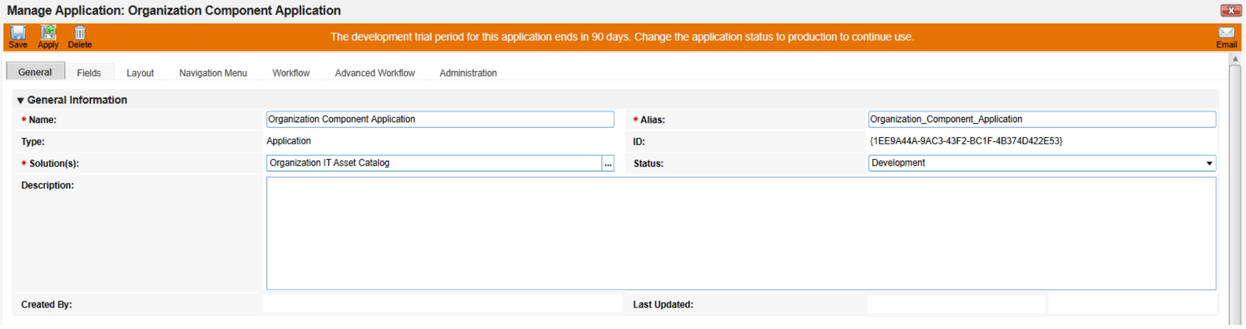
* Solution(s):

* Language:

* Required

Available	Selected
Find:	Organization IT Asset Catalog
IT Asset Catalog	
IT Security Vulnerabilities Program	
Organization IT Asset Catalog	
SCA IT Asset Catalog	
Schedule Management	
Task Management	
Third Party Catalog	

4. Click **Save**.



Manage Application: Organization Component Application

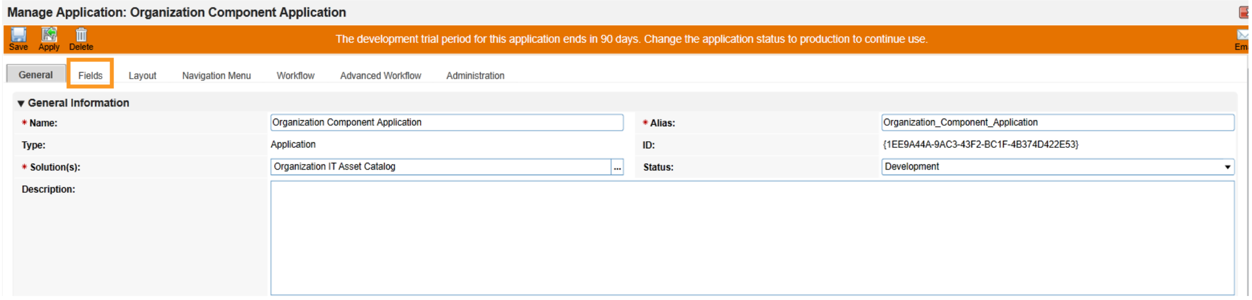
The development trial period for this application ends in 90 days. Change the application status to production to continue use.

General Information

* Name:	Organization Component Application	* Alias:	Organization_Component_Application
Type:	Application	ID:	{1EE9A44A-9AC3-43F2-BC1F-4B374D422E53}
* Solution(s):	Organization IT Asset Catalog	Status:	Development
Description:			
Created By:		Last Updated:	

In the next series of steps, we will add several Data Fields to the newly created application. These are like table columns you might define in a relational database. Note that we will only walk through one example, but the steps can be repeated for the remaining data fields. Before starting these steps, download and open the Components application schema from our repository. Some data fields, such as **Tracking ID**, **First Published**, and **Last Updated** are automatically created with each new application and do not need to be repeated.

5. Open the target Components application from the Administration menu under **Application Builder -> Applications**.
6. Click the **Fields** tab.



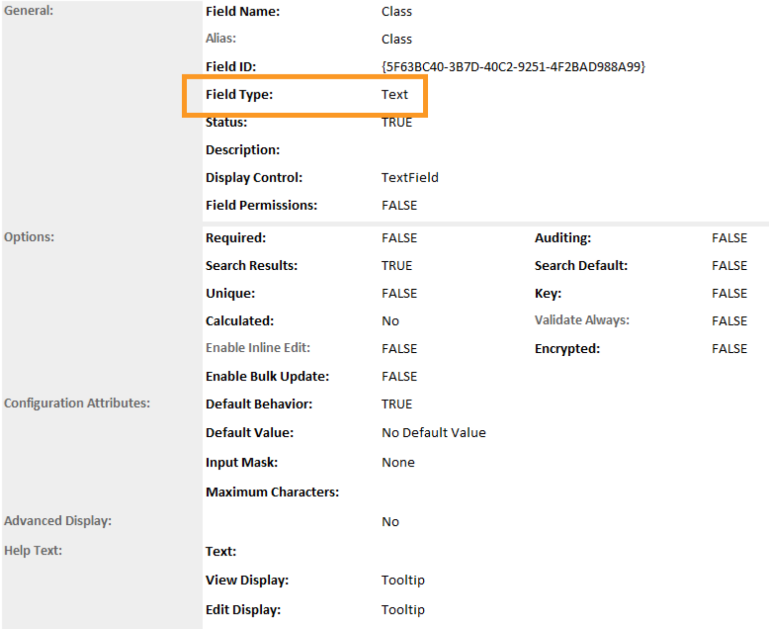
Manage Application: Organization Component Application

The development trial period for this application ends in 90 days. Change the application status to production to continue use.

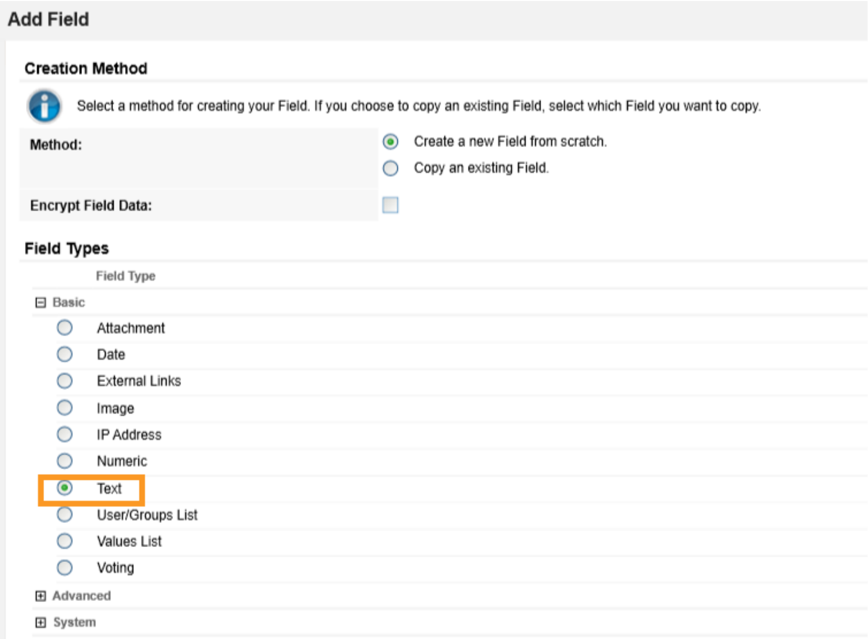
▼ General Information

* Name:	Organization Component Application	* Alias:	Organization_Component_Application
Type:	Application	ID:	{1EE9A44A-9AC3-43F2-BC1F-4B374D422E53}
* Solution(s):	Organization IT Asset Catalog	Status:	Development
Description:			

7. Click **Add New**. Match the Field Type from the spreadsheet to the **Field Type** field in RSA Archer. Click **OK**.



General:	Field Name:	Class		
	Alias:	Class		
	Field ID:	{5F63BC40-3B7D-40C2-9251-4F2BAD988A99}		
	Field Type:	Text		
	Status:	TRUE		
	Description:			
	Display Control:	TextField		
	Field Permissions:	FALSE		
Options:	Required:	FALSE	Auditing:	FALSE
	Search Results:	TRUE	Search Default:	FALSE
	Unique:	FALSE	Key:	FALSE
	Calculated:	No	Validate Always:	FALSE
	Enable Inline Edit:	FALSE	Encrypted:	FALSE
	Enable Bulk Update:	FALSE		
Configuration Attributes:	Default Behavior:	TRUE		
	Default Value:	No Default Value		
	Input Mask:	None		
	Maximum Characters:			
Advanced Display:		No		
Help Text:	Text:			
	View Display:	Tooltip		
	Edit Display:	Tooltip		



Add Field

Creation Method

Select a method for creating your Field. If you choose to copy an existing Field, select which Field you want to copy.

Method: ● Create a new Field from scratch. ○ Copy an existing Field.

Encrypt Field Data: □

Field Types

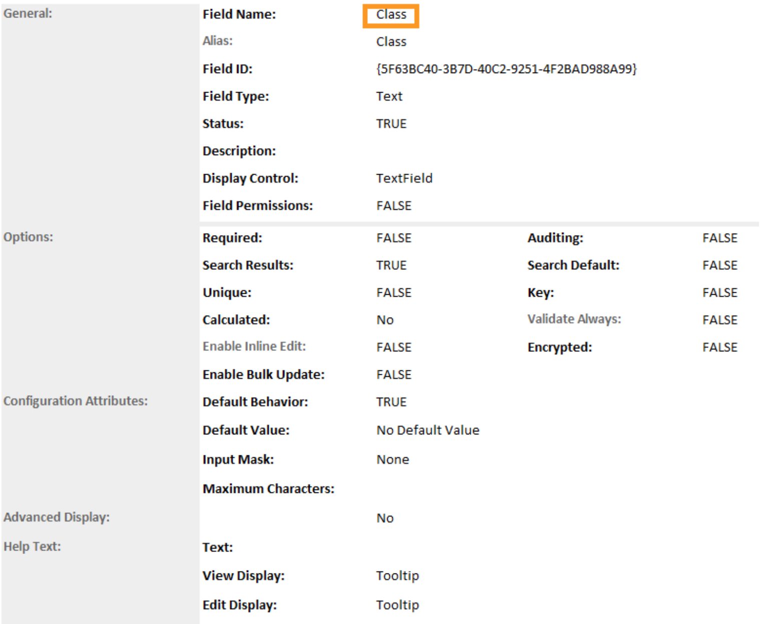
Field Type

⊟ Basic
- ○ Attachment
- ○ Date
- ○ External Links
- ○ Image
- ○ IP Address
- ○ Numeric
- ● Text
- ○ User/Groups List
- ○ Values List
- ○ Voting

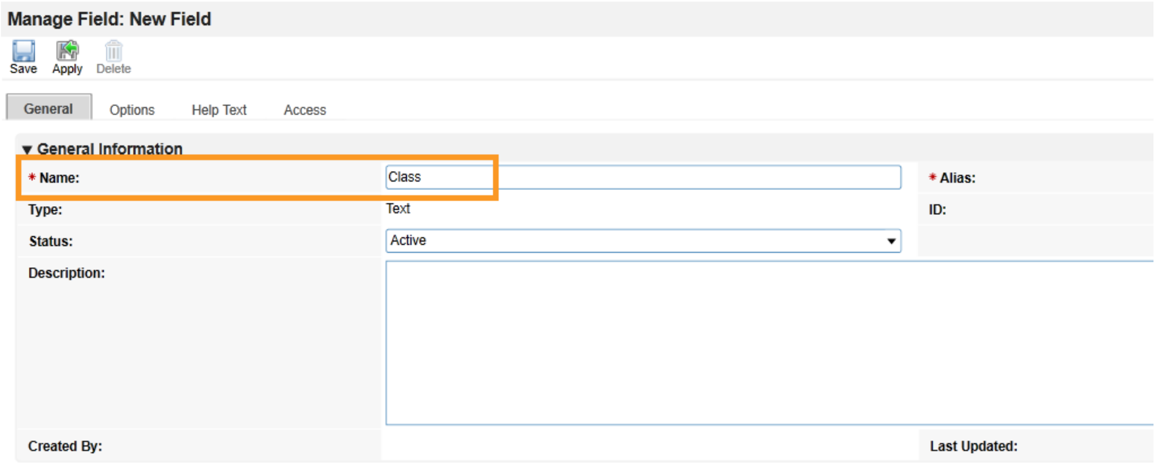
⊞ Advanced

⊞ System

8. Match the **Field Name** from the spreadsheet to the **Field Name** field in RSA Archer. Click **Save**.



General:	Field Name:	Class		
	Alias:	Class		
	Field ID:	{5F63BC40-3B7D-40C2-9251-4F2BAD988A99}		
	Field Type:	Text		
	Status:	TRUE		
	Description:			
	Display Control:	TextField		
	Field Permissions:	FALSE		
Options:	Required:	FALSE	Auditing:	FALSE
	Search Results:	TRUE	Search Default:	FALSE
	Unique:	FALSE	Key:	FALSE
	Calculated:	No	Validate Always:	FALSE
	Enable Inline Edit:	FALSE	Encrypted:	FALSE
	Enable Bulk Update:	FALSE		
Configuration Attributes:	Default Behavior:	TRUE		
	Default Value:	No Default Value		
	Input Mask:	None		
	Maximum Characters:			
Advanced Display:		No		
Help Text:	Text:			
	View Display:	Tooltip		
	Edit Display:	Tooltip		



* Name: Class

* Alias:

Type: Text

ID:

Status: Active

Description:

Created By:

Last Updated:

9. Repeat this process for all remaining data fields in the spreadsheet. Refer to the online documentation for other data types that might require additional configuration.

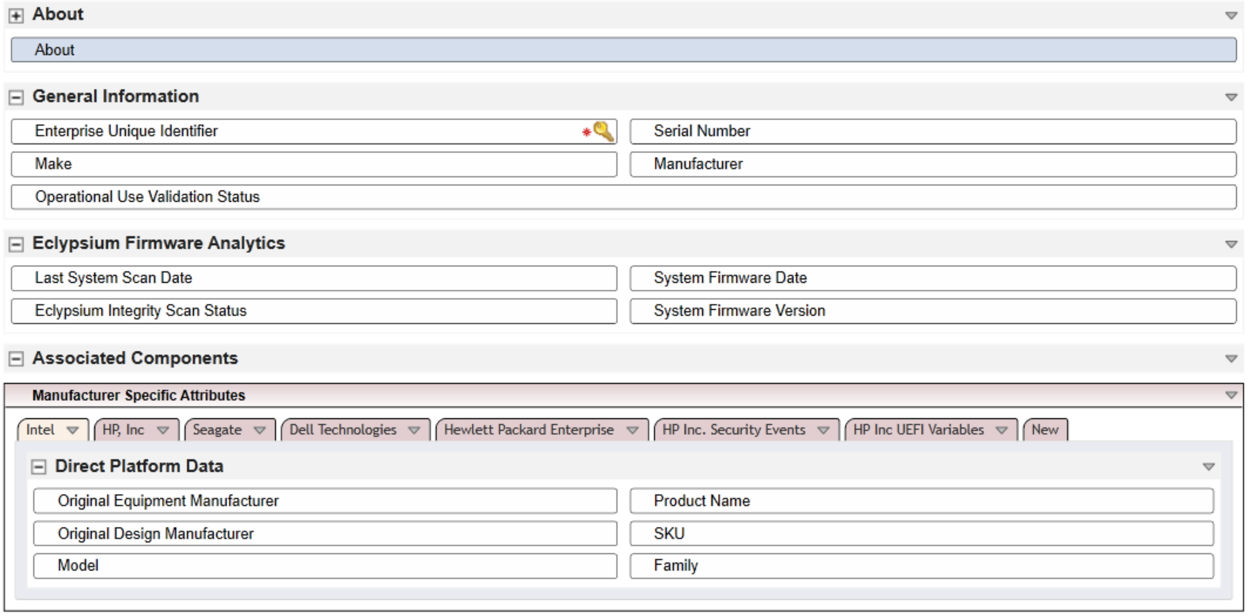
At this point, you have created the first supporting application for the Asset Discovery and Inventory system. Repeat these procedures to create the *HP Security Events* and *HP UEFI Configuration Variables* applications. These applications support the demonstration's dashboard capability related to HP Inc.'s security features that protect device integrity throughout the supply chain.

2.10.2.1.2 Modify Default *Devices* Application

In the next series of steps, modify the *Devices* with custom data fields that support the capabilities of this demonstration. You will also link this application to the supporting applications created in Section 2.10.2.1.1.

1. Using the Devices spreadsheet in our repository, add the custom data fields using the same method as described in Section 2.10.2.1.1. Note that cross-referenced data fields are links that will automatically create a new data field in the associated application.

2. Modify the layout of the Devices application to include data field customizations created in this section. The layout will be used to display detailed information about a computing device that has completed the acceptance testing process. Of note, we have added three sections – *General Information*, *Eclypsium Firmware Analytics*, and *Associated Components*. Use the screenshots below as a starting point for customizations that fit into your organization's workflow. More information regarding layouts can be found on RSA's website.



⊞ About

About

⊟ General Information

Enterprise Unique Identifier *

Serial Number

Make

Manufacturer

Operational Use Validation Status

⊟ Eclypsium Firmware Analytics

Last System Scan Date

System Firmware Date

Eclypsium Integrity Scan Status

System Firmware Version

⊟ Associated Components

Manufacturer Specific Attributes

⊟ Direct Platform Data

Original Equipment Manufacturer

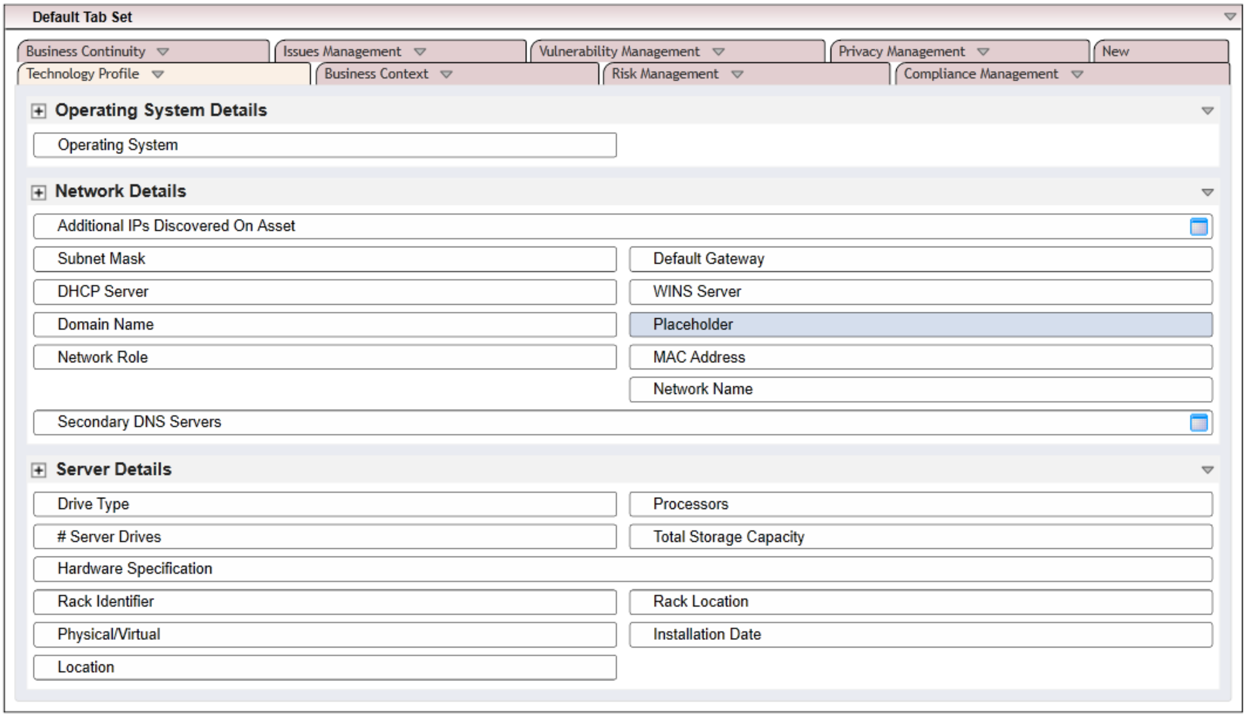
Product Name

Original Design Manufacturer

SKU

Model

Family



Default Tab Set

⊞ Operating System Details

Operating System

⊞ Network Details

Additional IPs Discovered On Asset

Subnet Mask

Default Gateway

DHCP Server

WINS Server

Domain Name

Placeholder

Network Role

MAC Address

Network Name

Secondary DNS Servers

⊞ Server Details

Drive Type

Processors

Server Drives

Total Storage Capacity

Hardware Specification

Rack Identifier

Rack Location

Physical/Virtual

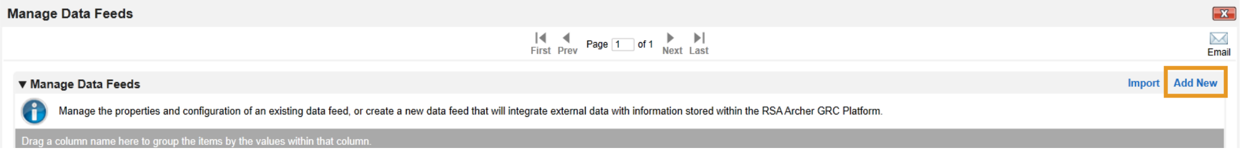
Installation Date

Location

2.10.2.2 Create Data Feed Integrations

In this section, the implementer will create *data feeds* in RSA Archer that will complete the integration with the PMCS, Microsoft Configuration Manager, and Eclypsium. The data feeds will periodically pull data from the three data sources and map it to the *Devices* application created in the preceding section.

1. In the Administration menu, navigate to **Integration -> Data Feeds**. Click **Add New**.

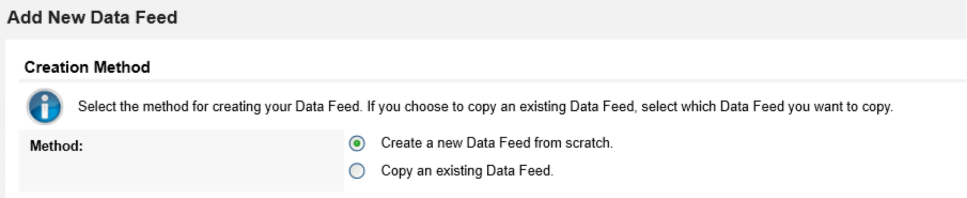


▼ Manage Data Feeds

Manage the properties and configuration of an existing data feed, or create a new data feed that will integrate external data with information stored within the RSA Archer GRC Platform.

Drag a column name here to group the items by the values within that column.

2. Select **Create a new Data Feed from scratch**. Click **OK**.

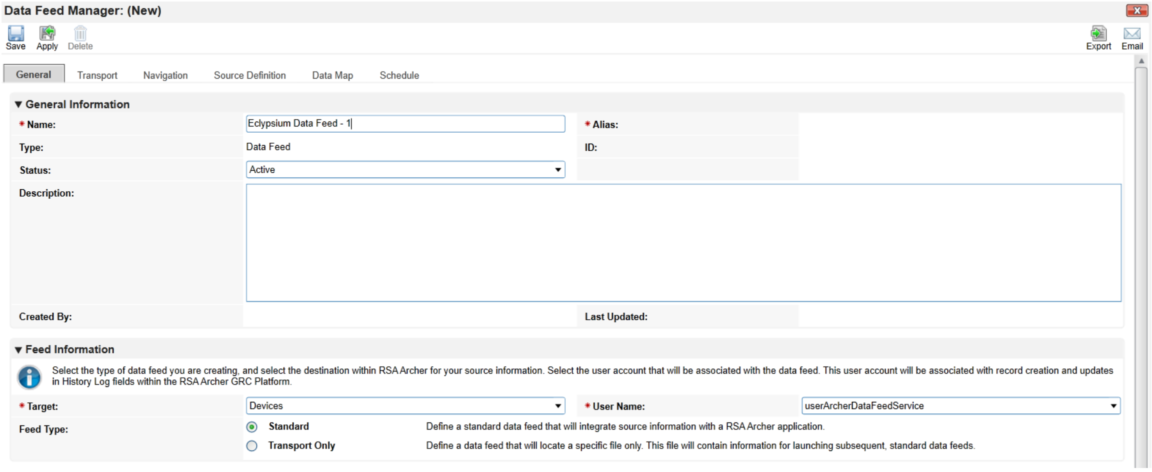


Creation Method

Select the method for creating your Data Feed. If you choose to copy an existing Data Feed, select which Data Feed you want to copy.

Method: ● Create a new Data Feed from scratch. ○ Copy an existing Data Feed.

3. Create an identifier in the **Name** field. Select the **Devices** application created in Section 2.10.2.1 in the **Target** field.



▼ General Information

* Name:	Eclypsium Data Feed - 1	* Alias:	
Type:	Data Feed	ID:	
Status:	Active		
Description:			
Created By:		Last Updated:	

▼ Feed Information

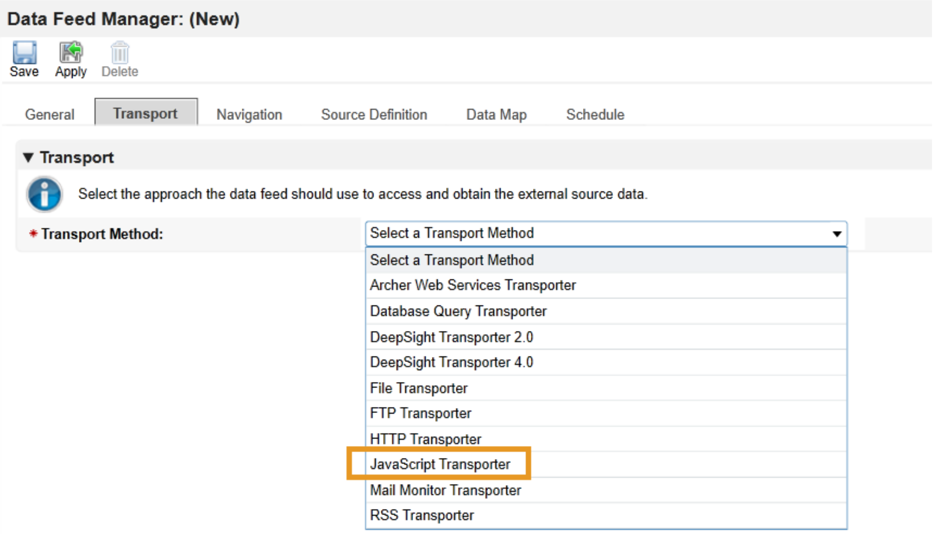
Select the type of data feed you are creating, and select the destination within RSA Archer for your source information. Select the user account that will be associated with the data feed. This user account will be associated with record creation and updates in History Log fields within the RSA Archer GRC Platform.

* Target: Devices

* User Name: userArcherDataFeedService

Feed Type:
● Standard — Define a standard data feed that will integrate source information with a RSA Archer application.
○ Transport Only — Define a data feed that will locate a specific file only. This file will contain information for launching subsequent, standard data feeds.

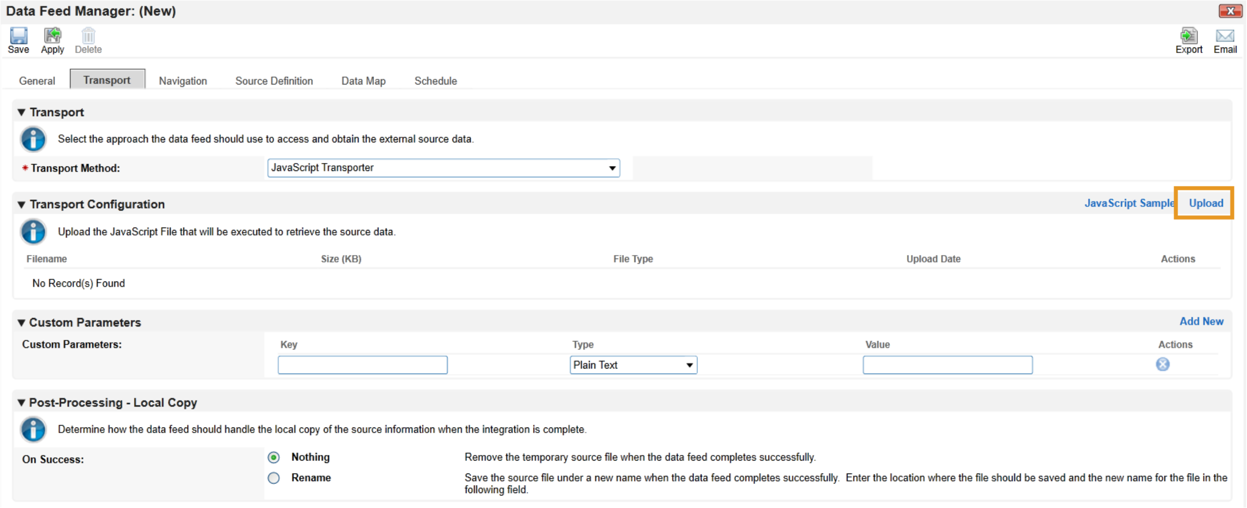
4. Click the **Transport** tab. Select **JavaScript Transporter**.



Select the approach the data feed should use to access and obtain the external source data.

* Transport Method: Select a Transport Method

5. Click **Upload** in the **Transport Configuration** section.



Select the approach the data feed should use to access and obtain the external source data.

* Transport Method: JavaScript Transporter

Upload the JavaScript File that will be executed to retrieve the source data.

No Record(s) Found

Custom Parameters: Type: Plain Text

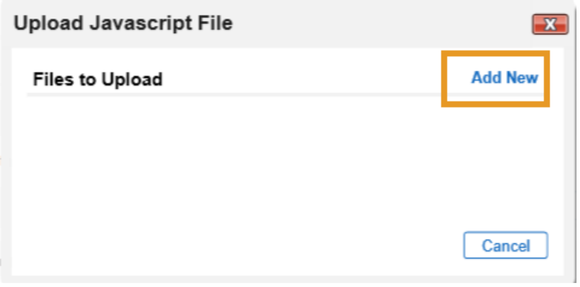
Determine how the data feed should handle the local copy of the source information when the integration is complete.

On Success:

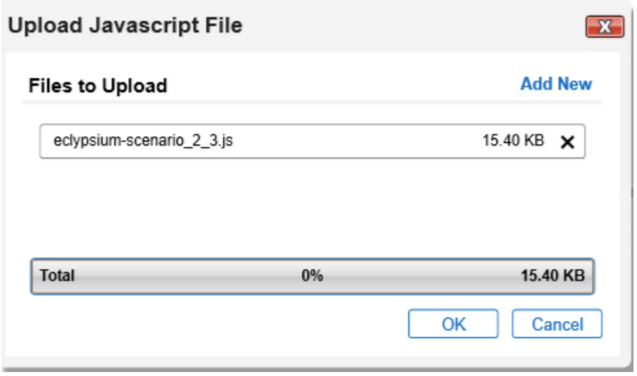
● Nothing — Remove the temporary source file when the data feed completes successfully.

○ Rename — Save the source file under a new name when the data feed completes successfully. Enter the location where the file should be saved and the new name for the file in the following field.

6. Click **Add New**.



7. In the file selection modal, select the Eclypsium JavaScript data feed file from the repository. Click **OK**.



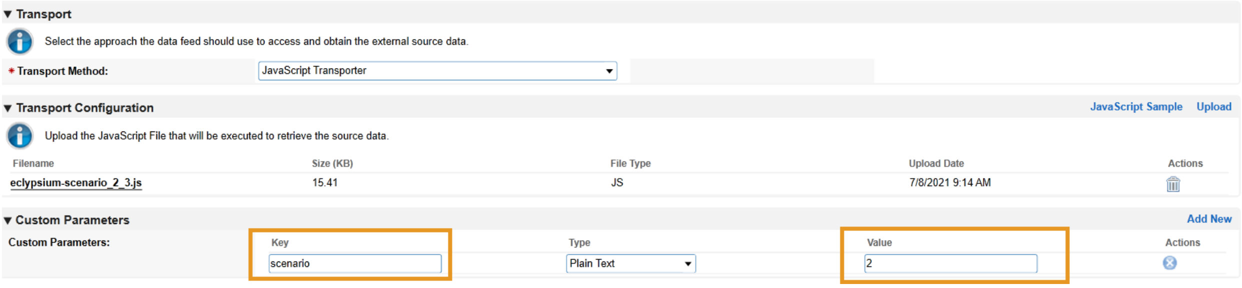
Upload Javascript File

Files to Upload

eclypsium-scenario_2_3.js 15.40 KB ✕

Total 0% 15.40 KB

8. Enter “scenario” in the **Key** field and “2” in the **Value** field.



▼ **Transport**

Select the approach the data feed should use to access and obtain the external source data.

* **Transport Method:** JavaScript Transporter

▼ **Transport Configuration**

Upload the JavaScript File that will be executed to retrieve the source data.

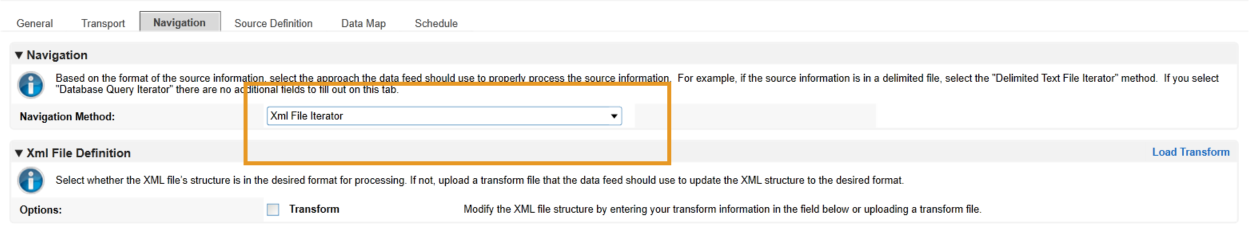
Filename	Size (KB)	File Type	Upload Date	Actions
eclypsium-scenario_2_3.js	15.41	JS	7/8/2021 9:14 AM	🗑

▼ **Custom Parameters**

Custom Parameters:

Key	Type	Value	Actions
scenario	Plain Text	2	⊗

9. Click the **Navigation** tab. Ensure **XML File Iterator** is selected in the **Navigation Method** dropdown menu.



▼ **Navigation**

Based on the format of the source information, select the approach the data feed should use to properly process the source information. For example, if the source information is in a delimited file, select the "Delimited Text File Iterator" method. If you select "Database Query Iterator" there are no additional fields to fill out on this tab.

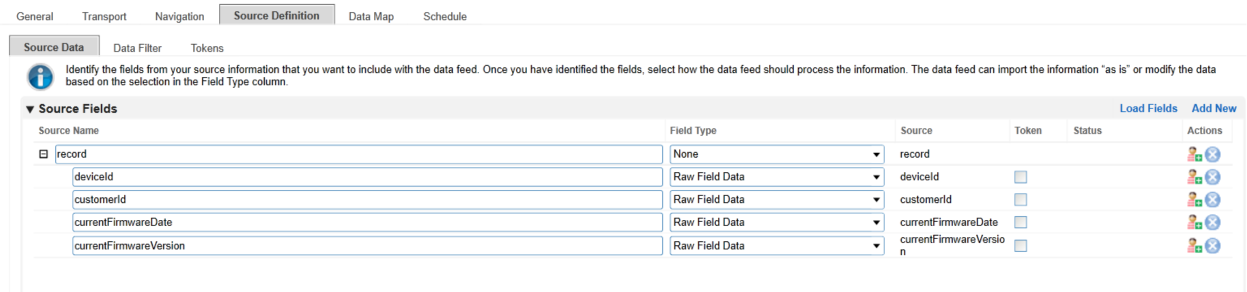
Navigation Method: Xml File Iterator

▼ **Xml File Definition**

Select whether the XML file's structure is in the desired format for processing. If not, upload a transform file that the data feed should use to update the XML structure to the desired format.

Options: □ **Transform** Modify the XML file structure by entering your transform information in the field below or uploading a transform file.

10. Click the **Source Definition** tab. In the **Source Data** sub-tab, select **Load Fields**. Select the Eclypsium example XML file. The configuration in Archer should populate the **Source Fields** as follows.

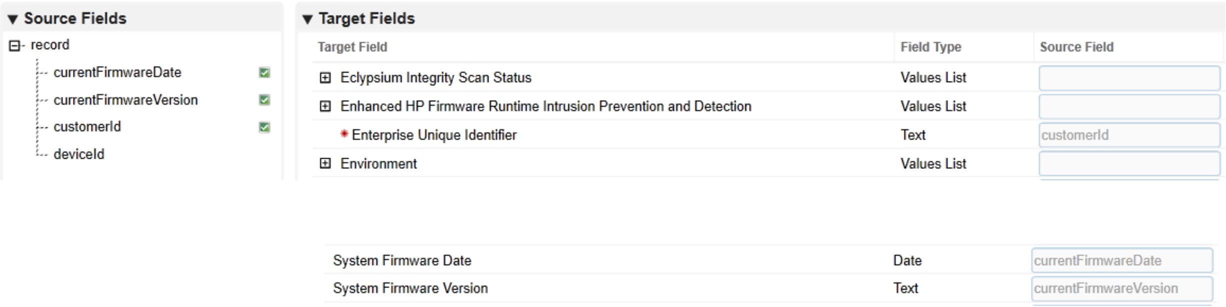


Identify the fields from your source information that you want to include with the data feed. Once you have identified the fields, select how the data feed should process the information. The data feed can import the information "as is" or modify the data based on the selection in the Field Type column.

▼ Source Fields

Source Name	Field Type	Source	Token	Status	Actions
⊟ record	None	record			
deviceId	Raw Field Data	deviceId	□		
customerId	Raw Field Data	customerId	□		
currentFirmwareDate	Raw Field Data	currentFirmwareDate	□		
currentFirmwareVersion	Raw Field Data	currentFirmwareVersion	□		

11. Click the **Data Map** and tab which will default to the **Field Map** sub-tab. Drag and drop the source fields onto the application data fields. Due to the large amount of data fields in the Devices application, below we present a truncated view of the mapping.

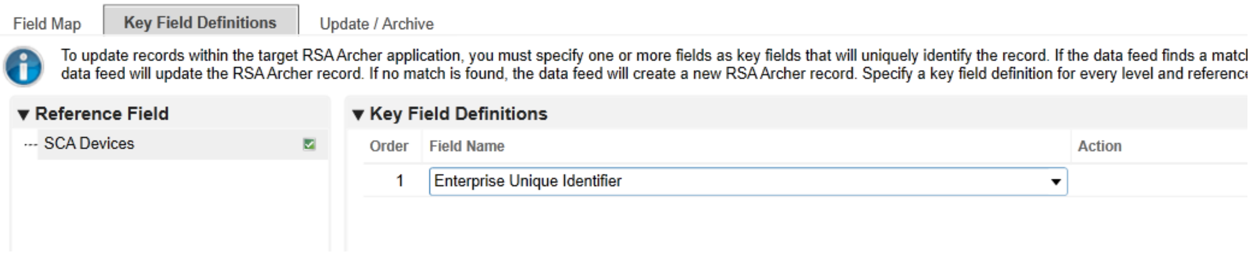

▼ Source Fields

⊟ record
- currentFirmwareDate ✓
- currentFirmwareVersion ✓
- customerId ✓
- deviceId

▼ Target Fields

Target Field	Field Type	Source Field
⊞ Eclypsium Integrity Scan Status	Values List	
⊞ Enhanced HP Firmware Runtime Intrusion Prevention and Detection	Values List	
* Enterprise Unique Identifier	Text	customerId
⊞ Environment	Values List	
System Firmware Date	Date	currentFirmwareDate
System Firmware Version	Text	currentFirmwareVersion

12. Click the **Key Field Definitions** tab. Select **Enterprise Unique Identifier** in the Field Name column.



To update records within the target RSA Archer application, you must specify one or more fields as key fields that will uniquely identify the record. If the data feed finds a matcl data feed will update the RSA Archer record. If no match is found, the data feed will create a new RSA Archer record. Specify a key field definition for every level and referenc

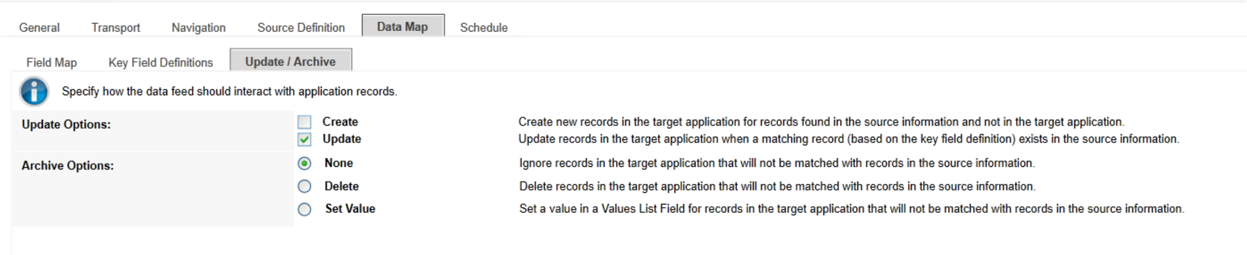
▼ Reference Field

--- SCA Devices ✓

▼ Key Field Definitions

Order	Field Name	Action
1	Enterprise Unique Identifier	

13. Click the **Update / Archive** tab. Ensure only the **Update** option is selected. Choose **None** for the **Archive Options**.

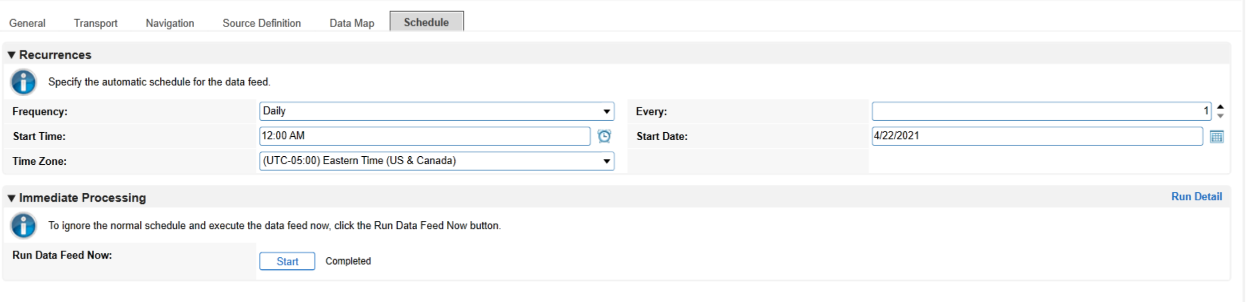


Specify how the data feed should interact with application records.

Update Options:
- □ Create — Create new records in the target application for records found in the source information and not in the target application.
- ☑ Update — Update records in the target application when a matching record (based on the key field definition) exists in the source information.

Archive Options:
- ● None — Ignore records in the target application that will not be matched with records in the source information.
- ○ Delete — Delete records in the target application that will not be matched with records in the source information.
- ○ Set Value — Set a value in a Values List Field for records in the target application that will not be matched with records in the source information.

14. Click the **Schedule** tab. Select a cadence appropriate for your organization. In this example, we've chosen to run the data feed on a daily frequency at 12:00AM.



▼ Recurrences

Specify the automatic schedule for the data feed.

Frequency: Daily

Every: 1

Start Time: 12:00 AM

Start Date: 4/22/2021

Time Zone: (UTC-05:00) Eastern Time (US & Canada)

▼ Immediate Processing

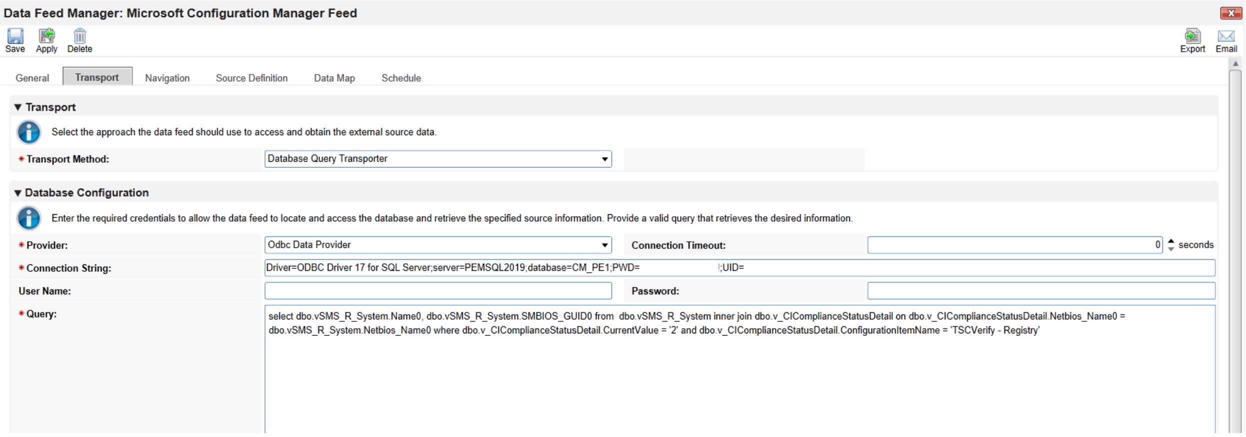
To ignore the normal schedule and execute the data feed now, click the Run Data Feed Now button.

Run Data Feed Now: Completed

At this point, the data feed for Eclypsium is configured. Click the **Start** button to confirm that the data feed has been properly configured. RSA Archer will report any errors that are useful for debugging. Repeat the preceding steps to add the Microsoft Configuration Manager Data Feed with the following modifications:

15. In the **Transport** tab, select **Database Query Transporter**. Insert the following values in the form:

Provider	`Odbc Data Provider`
Connection String	`Driver=ODBC Driver 17 for SQL Server;server=PEMSQL2019;database=CM_PE1;PWD=[SQL USER PASSWORD];UID=[SQL USER]`
Query	`select dbo.vSMS_R_System.Name0, dbo.vSMS_R_System.SMBIOS_GUID0 from dbo.vSMS_R_System inner join dbo.v_CIComplianceStatusDetail on dbo.v_CIComplianceStatusDetail.Netbios_Name0 = dbo.vSMS_R_System.Netbios_Name0 where dbo.v_CIComplianceStatusDetail.CurrentValue = '2' and dbo.v_CIComplianceStatusDetail.ConfigurationItemName = 'TSCVerify - Registry'`



Data Feed Manager: Microsoft Configuration Manager Feed

▼ Transport

Select the approach the data feed should use to access and obtain the external source data.

* Transport Method: Database Query Transporter

▼ Database Configuration

Enter the required credentials to allow the data feed to locate and access the database and retrieve the specified source information. Provide a valid query that retrieves the desired information.

* Provider: Odbc Data Provider

Connection Timeout: 0 seconds

* Connection String: Driver=ODBC Driver 17 for SQL Server;server=PEMSQL2019;database=CM_PE1;PWD= ;UID=

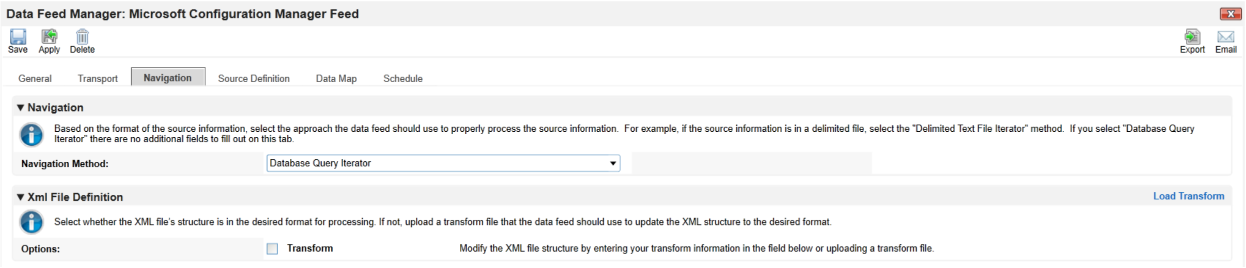
User Name:

Password:

* Query:

```
select dbo.vSMS_R_System.Name0, dbo.vSMS_R_System.SMBIOS_GUID0 from  dbo.vSMS_R_System inner join dbo.v_CIComplianceStatusDetail on dbo.v_CIComplianceStatusDetail.Netbios_Name0 =
dbo.vSMS_R_System.Netbios_Name0 where dbo.v_CIComplianceStatusDetail.CurrentValue = '2' and dbo.v_CIComplianceStatusDetail.ConfigurationItemName = 'TSCVerify - Registry'
```

16. In the **Navigation** tab, select **Database Query Iterator**.



Data Feed Manager: Microsoft Configuration Manager Feed

▼ Navigation

Based on the format of the source information, select the approach the data feed should use to properly process the source information. For example, if the source information is in a delimited file, select the "Delimited Text File Iterator" method. If you select "Database Query Iterator" there are no additional fields to fill out on this tab.

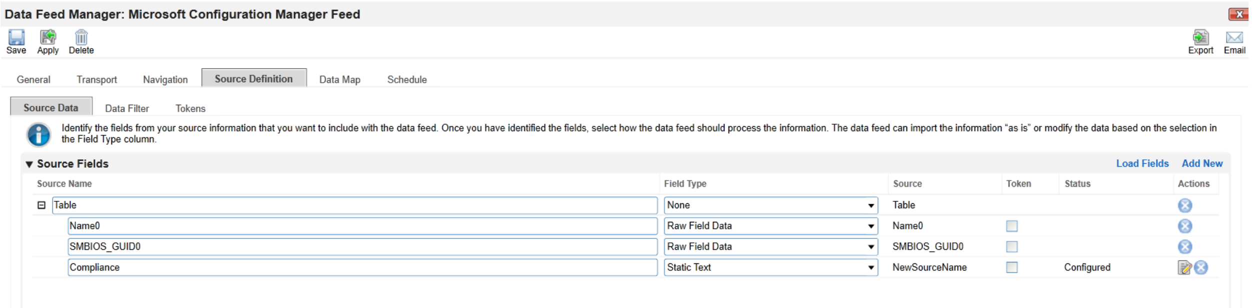
Navigation Method: Database Query Iterator

▼ Xml File Definition

Select whether the XML file's structure is in the desired format for processing. If not, upload a transform file that the data feed should use to update the XML structure to the desired format.

Options: □ Transform Modify the XML file structure by entering your transform information in the field below or uploading a transform file.

17. In the **Source Definition** tab, add a new **Source Field** named Compliance.



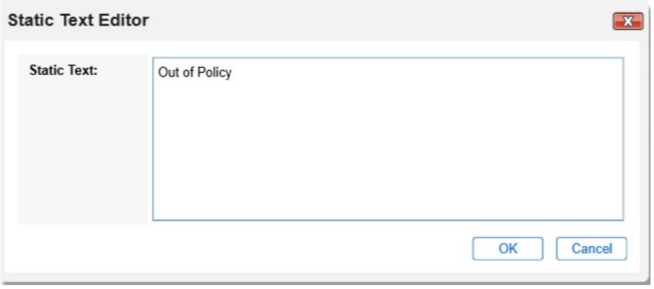
Data Feed Manager: Microsoft Configuration Manager Feed

Identify the fields from your source information that you want to include with the data feed. Once you have identified the fields, select how the data feed should process the information. The data feed can import the information "as is" or modify the data based on the selection in the Field Type column.

▼ Source Fields

Source Name	Field Type	Source	Token	Status	Actions
⊟ Table	None	Table			
Name0	Raw Field Data	Name0	□		
SMBIOS_GUID0	Raw Field Data	SMBIOS_GUID0	□		
Compliance	Static Text	NewSourceName	□	Configured	

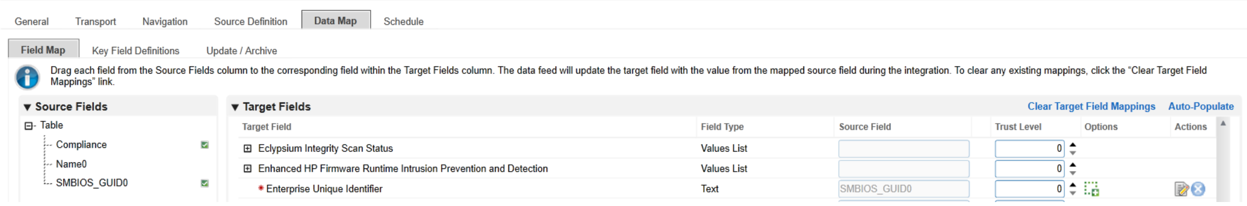
18. Edit the new **Source Field** with the static text "Out of Policy".



Static Text Editor

Static Text: Out of Policy

19. In the **Field Map** sub-tab in the **Data Map** tab, drag and drop the **Source Fields** onto the **Target Fields** as shown in the images below.



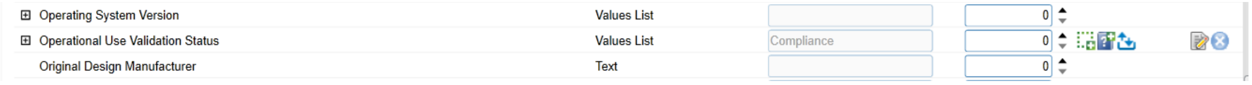
Drag each field from the Source Fields column to the corresponding field within the Target Fields column. The data feed will update the target field with the value from the mapped source field during the integration. To clear any existing mappings, click the "Clear Target Field Mappings" link.

▼ Source Fields

⊟ Table
- Compliance ✓
- Name0
- SMBIOS_GUID0 ✓

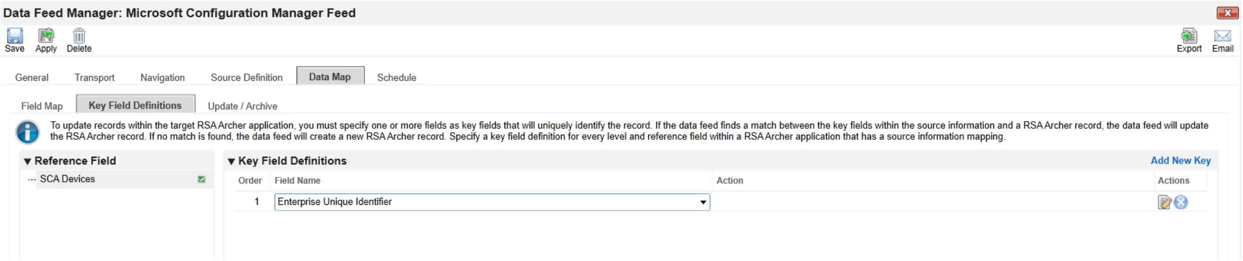
▼ Target Fields

Target Field	Field Type	Source Field	Trust Level	Options	Actions
⊞ Eclypsium Integrity Scan Status	Values List		0		
⊞ Enhanced HP Firmware Runtime Intrusion Prevention and Detection	Values List		0		
* Enterprise Unique Identifier	Text	SMBIOS_GUID0	0		



⊞ Operating System Version	Values List		0
⊞ Operational Use Validation Status	Values List	Compliance	0
Original Design Manufacturer	Text		0

20. In the **Key Field Definitions** sub-tab in the **Data Map** tab, select **Enterprise Unique Identifier**.



Data Feed Manager: Microsoft Configuration Manager Feed

To update records within the target RSA Archer application, you must specify one or more fields as key fields that will uniquely identify the record. If the data feed finds a match between the key fields within the source information and a RSA Archer record, the data feed will update the RSA Archer record. If no match is found, the data feed will create a new RSA Archer record. Specify a key field definition for every level and reference field within a RSA Archer application that has a source information mapping.

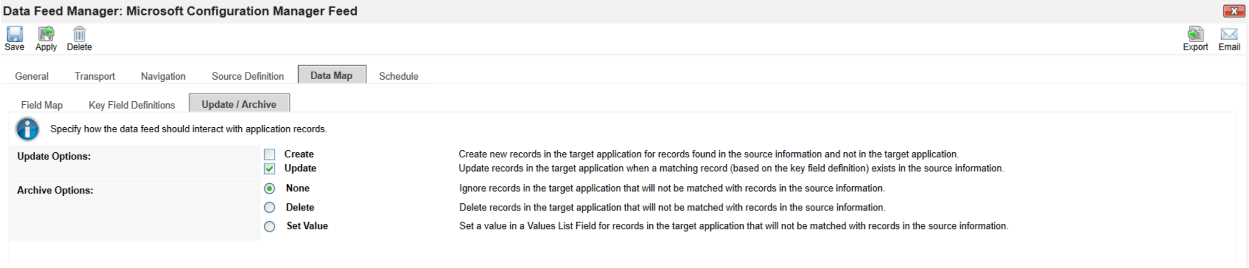
▼ Reference Field

--- SCA Devices ☑

▼ Key Field Definitions — Add New Key

Order	Field Name	Action	Actions
1	Enterprise Unique Identifier		

21. In the **Update / Archive** sub-tab in the **Data Map** tab, ensure only Update is selected.



Data Feed Manager: Microsoft Configuration Manager Feed

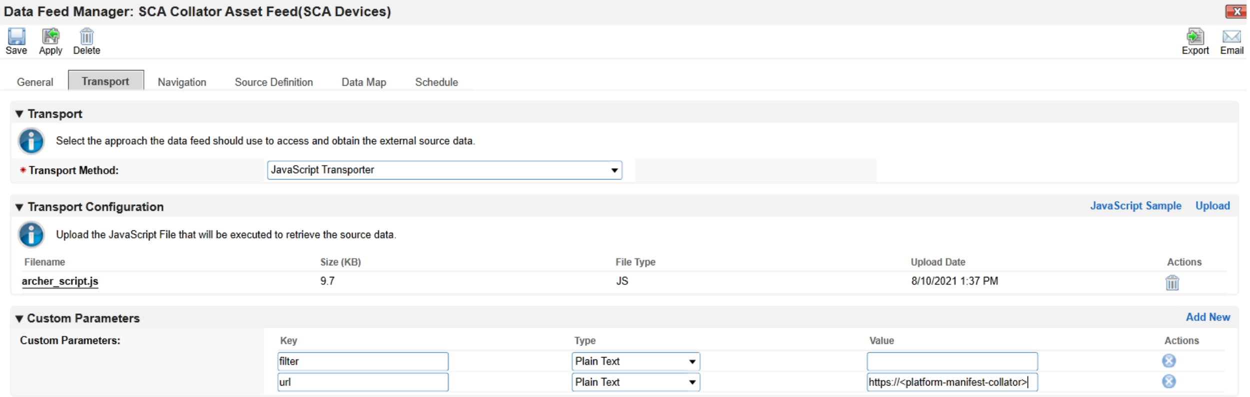
Specify how the data feed should interact with application records.

Update Options:
- □ Create — Create new records in the target application for records found in the source information and not in the target application.
- ☑ Update — Update records in the target application when a matching record (based on the key field definition) exists in the source information.

Archive Options:
- ● None — Ignore records in the target application that will not be matched with records in the source information.
- ○ Delete — Delete records in the target application that will not be matched with records in the source information.
- ○ Set Value — Set a value in a Values List Field for records in the target application that will not be matched with records in the source information.

At this point, the Data Feed for the Microsoft Configuration Manager is configured. Click the **Start** button to confirm that the Data Feed has been properly configured. Archer will report any errors that are useful for debugging. Repeat the initial steps to add the final DataFeed for the PMCS with the following modifications:

22. In the Transport tab, upload the custom JavaScript from the project repository. In the Custom Parameters fields, add a **filter** and **URL** Key as shown below. The value for **filter** may be blank or set to a specific manufacturer (refer to comments in the script for the specific values we used). Set **URL** to the location of the PMCS in your environment.



Data Feed Manager: SCA Collator Asset Feed(SCA Devices)

▼ Transport

Select the approach the data feed should use to access and obtain the external source data.

* Transport Method: JavaScript Transporter

▼ Transport Configuration

Upload the JavaScript File that will be executed to retrieve the source data.

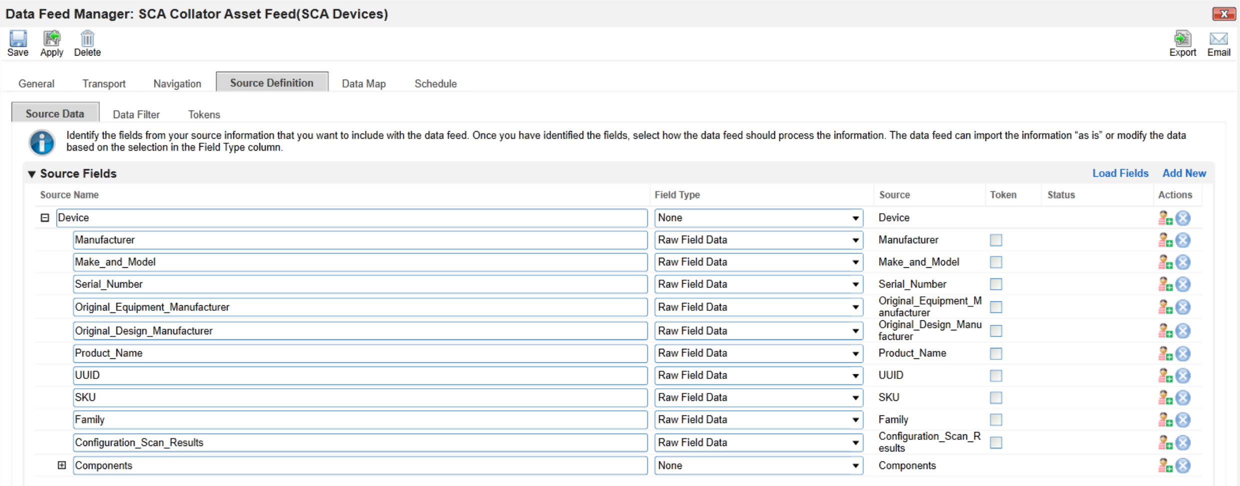
Filename	Size (KB)	File Type	Upload Date	Actions
archer_script.js	9.7	JS	8/10/2021 1:37 PM	

▼ Custom Parameters

Custom Parameters:

Key	Type	Value	Actions
filter	Plain Text		
url	Plain Text	https://<platform-manifest-collator>	

23. In the **Source Definition** tab, upload the example XML file from the project repository. The **Source Fields** should resemble the following screenshot.



Data Feed Manager: SCA Collator Asset Feed(SCA Devices)

Identify the fields from your source information that you want to include with the data feed. Once you have identified the fields, select how the data feed should process the information. The data feed can import the information “as is” or modify the data based on the selection in the Field Type column.

▼ Source Fields

Source Name	Field Type	Source	Token	Status	Actions
⊟ Device	None	Device			
Manufacturer	Raw Field Data	Manufacturer	□		
Make_and_Model	Raw Field Data	Make_and_Model	□		
Serial_Number	Raw Field Data	Serial_Number	□		
Original_Equipment_Manufacturer	Raw Field Data	Original_Equipment_Manufacturer	□		
Original_Design_Manufacturer	Raw Field Data	Original_Design_Manufacturer	□		
Product_Name	Raw Field Data	Product_Name	□		
UUID	Raw Field Data	UUID	□		
SKU	Raw Field Data	SKU	□		
Family	Raw Field Data	Family	□		
Configuration_Scan_Results	Raw Field Data	Configuration_Scan_Results	□		
⊞ Components	None	Components			

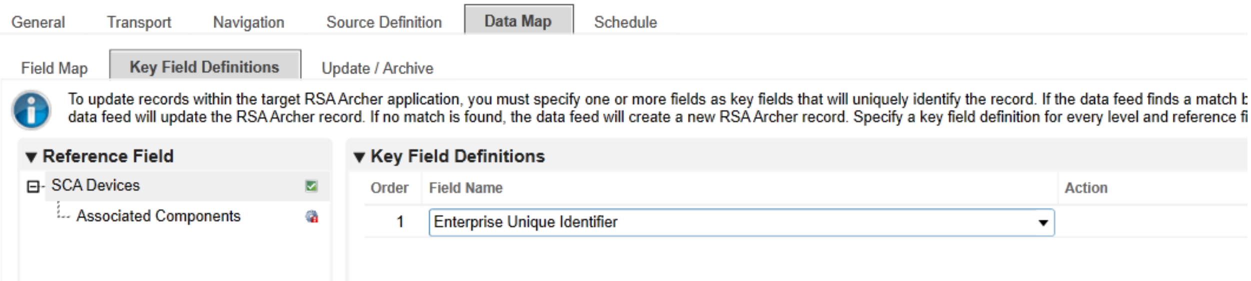
24. Map the **Source Fields** to the **Target Fields** and the **Field Map** sub-tab in the **Data Map** tab. Use Table 2-5 for reference.

Table 2-5 Source Field to Destination Field Mapping

Source Field	Destination Field
/Component/Addresses/Address	Associated Components/Addresses/Address
/Component/Class	Associated Components/Class
/Component/Field_Replaceable	Associated Components/Field Replaceable
/Component/Manufacturer	Associated Components/Manufacturer
/Component/Model	Associated Components/Model
/Component/Platform_Certificate	Associated Components/Platform Certificate
/Component/Platform_Certificate_URI	Associated Components/Platform Certificate URI
/Component/Revision	Associated Components/Revision
/Component/Serial	Associated Components/Serial
/Component/Version	Associated Components/Version
UUID	Enterprise Unique Identifier

Source Field	Destination Field
Family	Family
Make_and_Model	Make
Manufacturer	Manufacturer/Value
Original_Design_Manufacturer	Original Design Manufacturer
Original_Equipment_Manufacturer	Original Equipment Manufacturer
Product_Name	Product Name
Serial_Number	Serial Number
SKU	SKU

25. In the **Key Field Definitions** sub-tab in the **Data Map** tab, choose Enterprise Unique Identifier as the **Key Field** definition.



To update records within the target RSA Archer application, you must specify one or more fields as key fields that will uniquely identify the record. If the data feed finds a match b data feed will update the RSA Archer record. If no match is found, the data feed will create a new RSA Archer record. Specify a key field definition for every level and reference fi

Reference Field

- SCA Devices
  - Associated Components

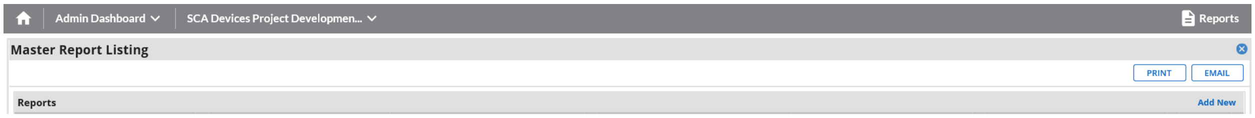
Key Field Definitions

Order	Field Name	Action
1	Enterprise Unique Identifier	

The Data Feed for the PMCS is configured. Click the **Start** button to confirm that the Data Feed has been properly configured. Archer will report any errors that are useful for debugging.

2.10.2.3 Create the Dashboard

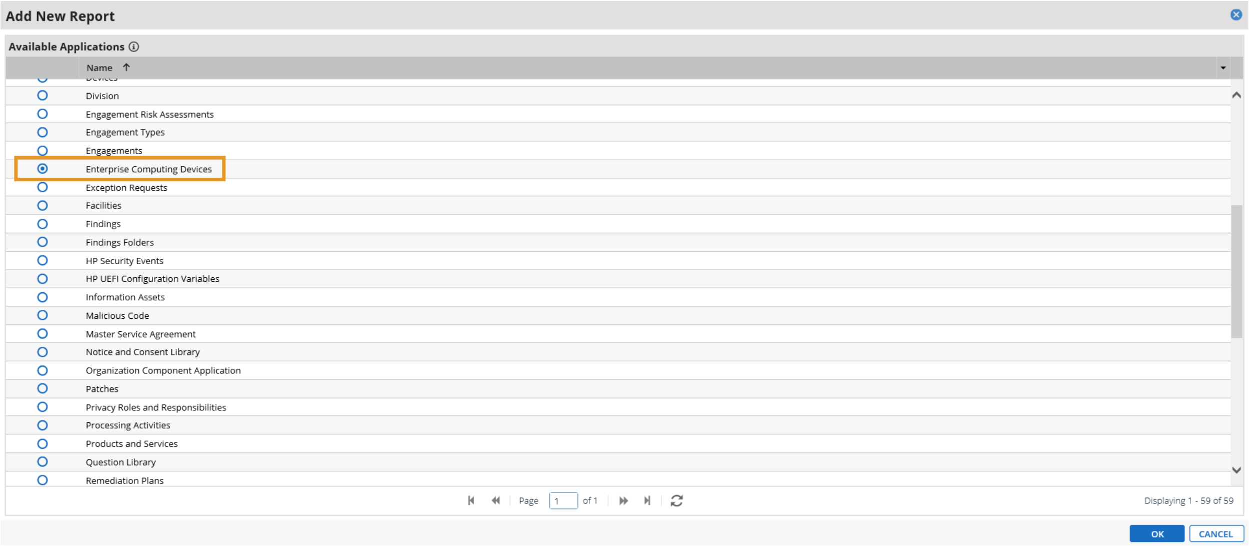
1. Create a new report by clicking Reports in the administrative console and **Add New**.



Master Report Listing

Reports

2. Select the Devices application that was created in the preceding steps—in this case, **Enterprise Computing Devices**.

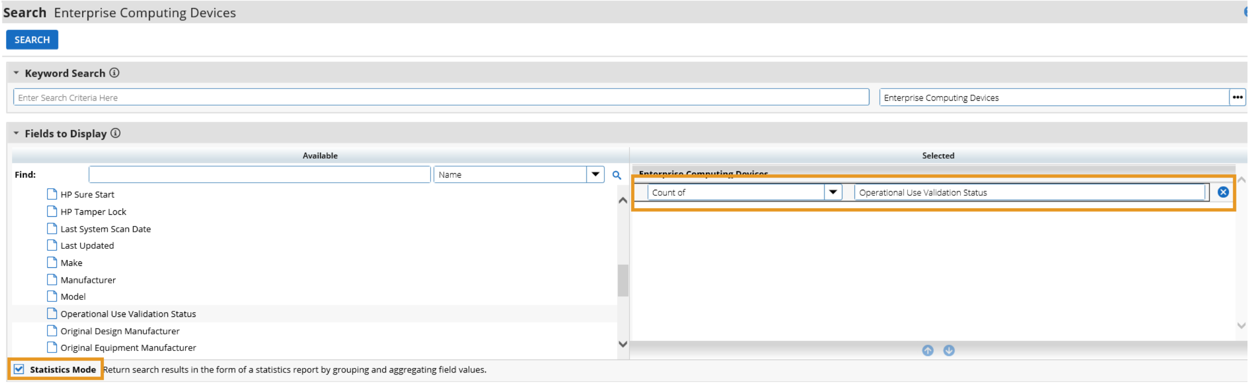


Add New Report

Available Applications

Name
○ Division
○ Engagement Risk Assessments
○ Engagement Types
○ Engagements
● Enterprise Computing Devices
○ Exception Requests
○ Facilities
○ Findings
○ Findings Folders
○ HP Security Events
○ HP UEFI Configuration Variables
○ Information Assets
○ Malicious Code
○ Master Service Agreement
○ Notice and Consent Library
○ Organization Component Application
○ Patches
○ Privacy Roles and Responsibilities
○ Processing Activities
○ Products and Services
○ Question Library
○ Remediation Plans

3. Click the Statistics Mode option. In the **Fields to Display** section, select **Operational Use Validation Status** and remove the default selections.



Search Enterprise Computing Devices

Enterprise Computing Devices

Fields to Display

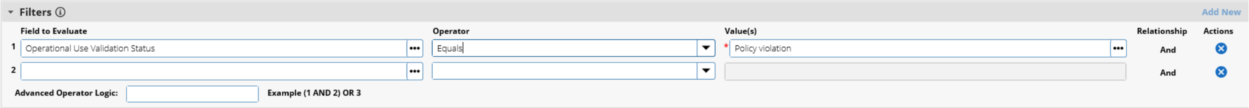
Available — Find: Name

- HP Sure Start
- HP Tamper Lock
- Last System Scan Date
- Last Updated
- Make
- Manufacturer
- Model
- Operational Use Validation Status
- Original Design Manufacturer
- Original Equipment Manufacturer

Selected — Enterprise Computing Devices: Count of | Operational Use Validation Status

☑ **Statistics Mode** Return search results in the form of a statistics report by grouping and aggregating field values.

4. In the **Filters** section, select *Operational Use Validation Status* for **Field to Evaluate**, *Equals* for **Operator**, and *Policy violation* from **Value(s)**.

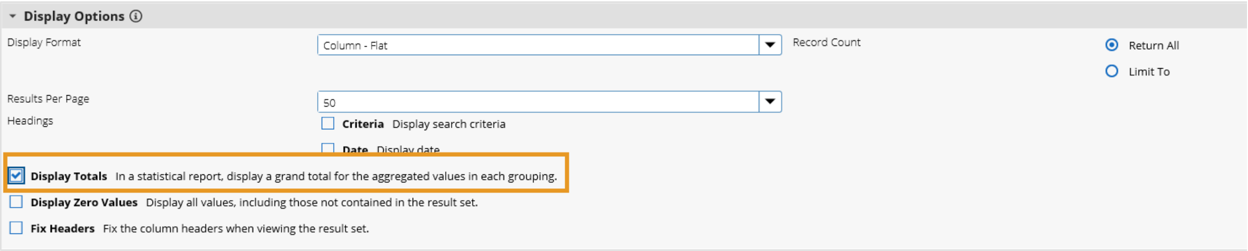


Filters

	Field to Evaluate	Operator	Value(s)	Relationship	Actions
1	Operational Use Validation Status	Equals	* Policy violation	And	⊗
2				And	⊗

Advanced Operator Logic: Example (1 AND 2) OR 3

5. Select **Display Totals** in the **Display Options** section.



Display Options ⓘ

Display Format: Column - Flat

Record Count: ● Return All ○ Limit To

Results Per Page: 50

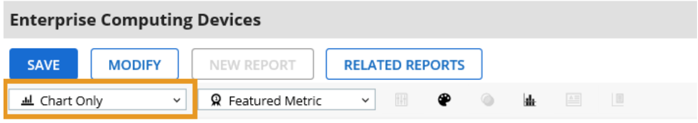
Headings: □ **Criteria** Display search criteria □ **Date** Display date

☑ **Display Totals** In a statistical report, display a grand total for the aggregated values in each grouping.

□ **Display Zero Values** Display all values, including those not contained in the result set.

□ **Fix Headers** Fix the column headers when viewing the result set.

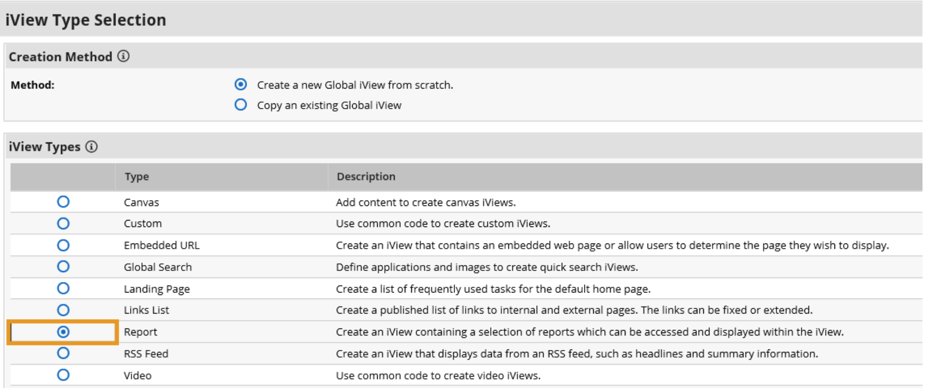
6. Select **Chart Only** and click **Save** and supply a unique name for the report.



Enterprise Computing Devices

7. Create a new iView by navigating to **Workspaces and Dashboards -> Global iViews** in the administrative menu. Click **Add New**.

8. In the **iView Types** section, select **Report** and click **OK**.



iView Type Selection

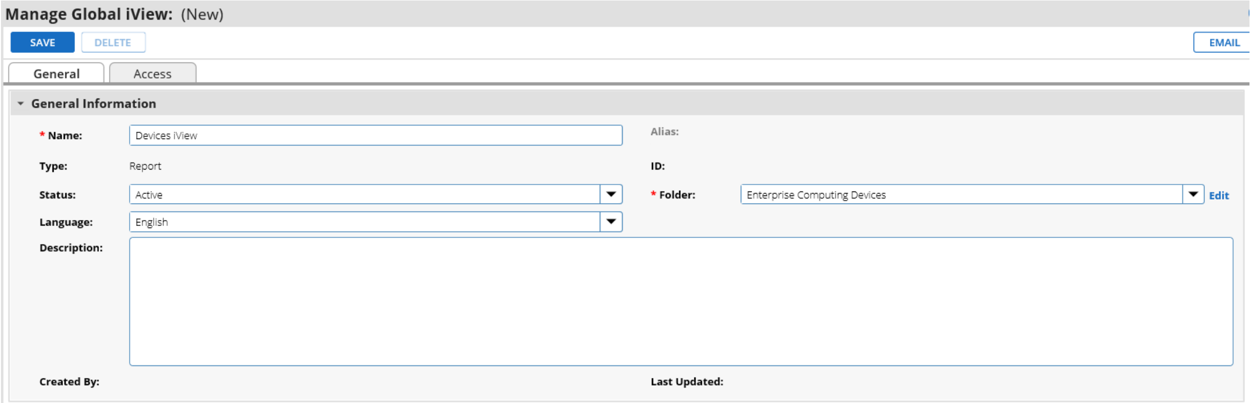
Creation Method ⓘ

Method: ● Create a new Global iView from scratch. ○ Copy an existing Global iView

iView Types ⓘ

	Type	Description
○	Canvas	Add content to create canvas iViews.
○	Custom	Use common code to create custom iViews.
○	Embedded URL	Create an iView that contains an embedded web page or allow users to determine the page they wish to display.
○	Global Search	Define applications and images to create quick search iViews.
○	Landing Page	Create a list of frequently used tasks for the default home page.
○	Links List	Create a published list of links to internal and external pages. The links can be fixed or extended.
●	Report	Create an iView containing a selection of reports which can be accessed and displayed within the iView.
○	RSS Feed	Create an iView that displays data from an RSS feed, such as headlines and summary information.
○	Video	Use common code to create video iViews.

9. In the **General Information** section, supply a name and a folder to store the new iView.



Manage Global iView: (New)

General Information

* **Name:** Devices iView

Alias:

Type: Report

ID:

Status: Active

* **Folder:** Enterprise Computing Devices

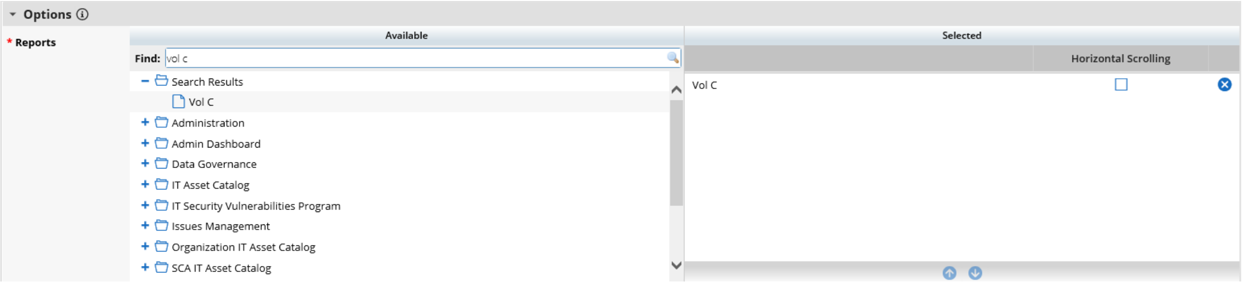
Language: English

Description:

Created By:

Last Updated:

10. In the **Options** section, choose the report that was created in the preceding steps and save the iView.



Options ⓘ

* Reports

Available

Find: vol c

− Search Results
- Vol C

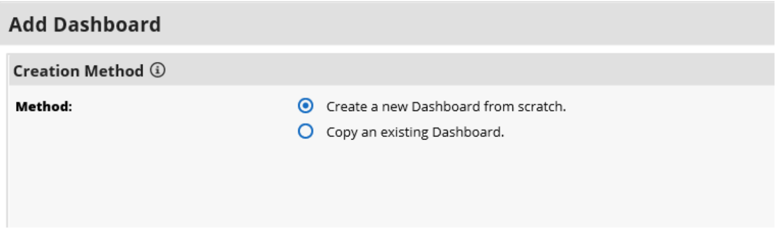
+ Administration
+ Admin Dashboard
+ Data Governance
+ IT Asset Catalog
+ IT Security Vulnerabilities Program
+ Issues Management
+ Organization IT Asset Catalog
+ SCA IT Asset Catalog

Selected

	Horizontal Scrolling
Vol C	☐

11. Create a new Dashboard by navigating to **Workspaces and Dashboards -> Dashboards** in the administration menu. Click **Add New**.

12. Select **Create a new Dashboard** from scratch and click **OK**.



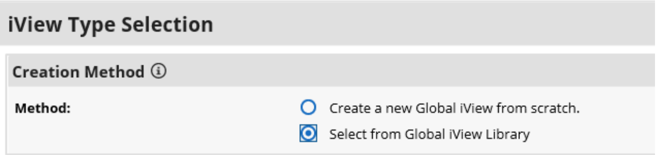
Add Dashboard

Creation Method ⓘ

Method: ● Create a new Dashboard from scratch.
○ Copy an existing Dashboard.

13. In the **General** tab, supply a name for the Dashboard.

14. In the **Layout** tab, click Select iViews. Choose Select from **Global iView Library** for the **Creation Method**. Choose the iView created in the preceding steps and click **OK**.

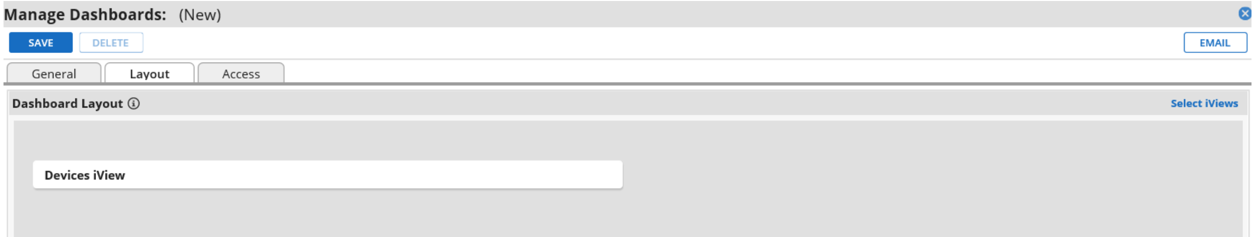


iView Type Selection

Creation Method ⓘ

Method: ○ Create a new Global iView from scratch.
● Select from Global iView Library

15. The selected iView will appear in the layout. Save the Dashboard.



Manage Dashboards: (New)

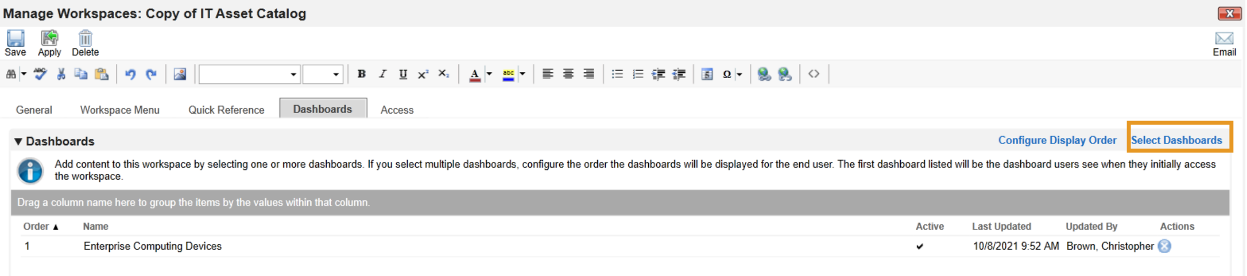
SAVE DELETE EMAIL

General Layout Access

Dashboard Layout ⓘ Select iViews

Devices iView

16. Open the solution workspace by navigating to Workspaces and **Dashboards -> Workspaces** in the administration menu. In the **Dashboards** tab, choose the Dashboard created in the preceding steps by clicking **Select Dashboards**.



Manage Workspaces: Copy of IT Asset Catalog

▼ Dashboards

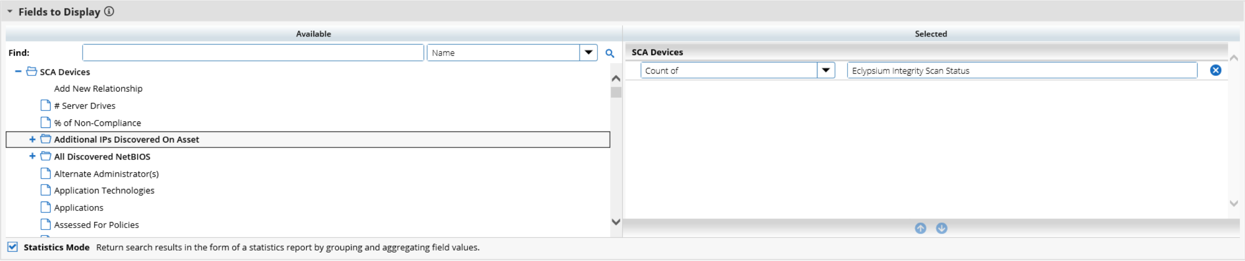
Add content to this workspace by selecting one or more dashboards. If you select multiple dashboards, configure the order the dashboards will be displayed for the end user. The first dashboard listed will be the dashboard users see when they initially access the workspace.

Drag a column name here to group the items by the values within that column.

Order ▲	Name	Active	Last Updated	Updated By	Actions
1	Enterprise Computing Devices	✓	10/8/2021 9:52 AM	Brown, Christopher	⊗

17. Save the workspace. At this point, the new Dashboard will appear as part of the workspace. For further customization options, refer to the RSA website.

18. Repeat the steps in this section to add a dashboard item that tracks platform integrity issues that are detected from the Eclypsium platform. Use the Eclypsium Integrity Scan Status data field while generating the new report.



SCA Devices: Count of — Eclypsium Integrity Scan Status

☑ **Statistics Mode** Return search results in the form of a statistics report by grouping and aggregating field values.

3 Operational Considerations

This section describes the execution steps of an IT administrator assigned to the acceptance testing or monitoring of computing devices during their operational lifecycle. Each subsection restates the scenarios from the project description, but this prototype demonstration does not address each scenario in totality. This preliminary draft will be updated later with additional guidance for laptops and servers.

Create an environment as described in Section 2 before attempting to use the proof-of-concept tools below.

3.1 Scenario 2: Verification of Components During Acceptance Testing

In this scenario, an IT administrator receives a computing device through nonverifiable channels (e.g., off the shelf at a retailer) and wishes to confirm its provenance and authenticity to establish an authoritative asset inventory as part of an asset management program.

The general execution steps are as follows:

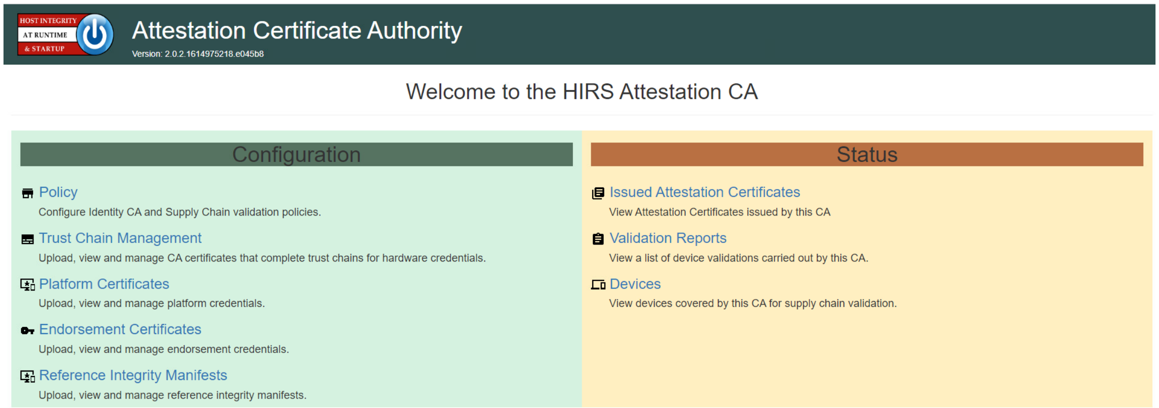
1. As part of the acceptance testing process, the IT administrator uses tools to extract or obtain the verifiable platform artifact associated with the computing device.
2. The IT administrator verifies the provenance of the device's hardware components by validating the source and authenticity of the artifact.
3. The IT administrator validates the verifiable artifact by interrogating the device to obtain platform attributes that can be compared against those listed in the artifact.
4. The computing device is provisioned into the physical asset management system and is associated with a unique enterprise identifier. If the administrator updates the configuration of the platform (e.g., adding hardware components, updating firmware), then the administrator might create new platform artifacts to establish a new baseline.

3.1.1 Technology Configurations

3.1.1.1 Configure the HIRS ACA

Before running the acceptance test on Dell and HP Inc. laptops, the HIRS-ACA must be configured with the target laptop's platform attribute certificate and any trust chains associated with the platform attribute certificate and endorsement credential.

1. On the HIRS ACA web portal, under the **Configuration** panel, select **Policy.**



Attestation Certificate Authority

Version: 2.0.2.1614975218.e045b8

Welcome to the HIRS Attestation CA

Configuration

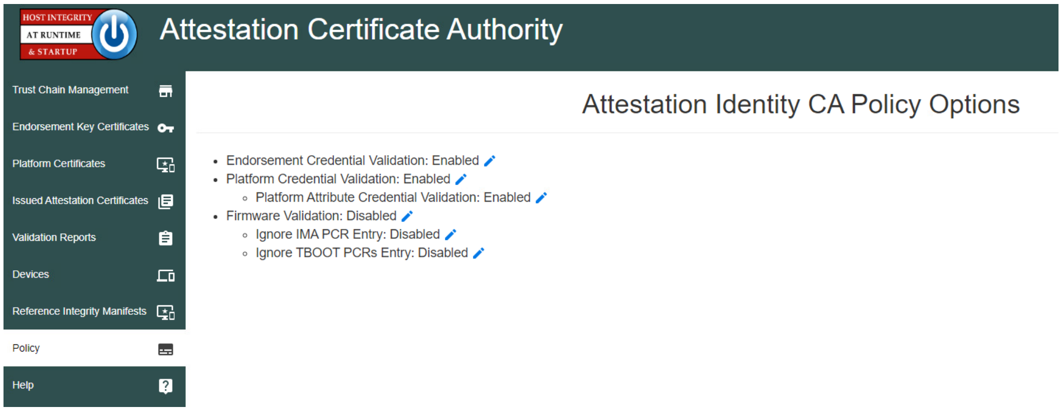
- Policy
  Configure Identity CA and Supply Chain validation policies.
- Trust Chain Management
  Upload, view and manage CA certificates that complete trust chains for hardware credentials.
- Platform Certificates
  Upload, view and manage platform credentials.
- Endorsement Certificates
  Upload, view and manage endorsement credentials.
- Reference Integrity Manifests
  Upload, view and manage reference integrity manifests.

Status

- Issued Attestation Certificates
  View Attestation Certificates issued by this CA
- Validation Reports
  View a list of device validations carried out by this CA.
- Devices
  View devices covered by this CA for supply chain validation.

2. For this prototype demonstration, make sure the following policy options are set as listed in the table below.

Policy Option	Setting
Endorsement Credential Validation	Enabled
Platform Credential Validation	Enabled
Platform Attribute Credential Validation	Enabled
Firmware Validation	Disabled
Ignore IMA PCR Entry	Disabled
Ignore TBOOT PCRs Entry	Disabled

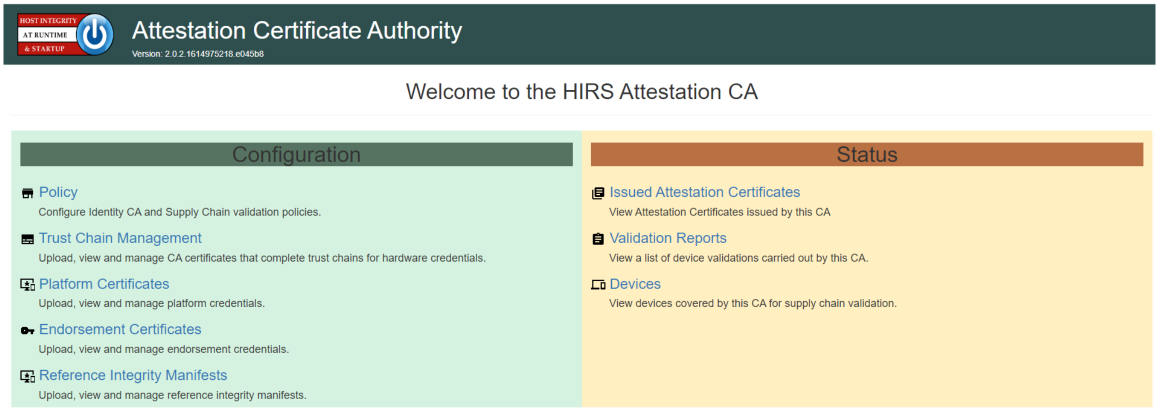


Attestation Certificate Authority

Attestation Identity CA Policy Options

- Endorsement Credential Validation: Enabled
- Platform Credential Validation: Enabled
    - Platform Attribute Credential Validation: Enabled
- Firmware Validation: Disabled
    - Ignore IMA PCR Entry: Disabled
    - Ignore TBOOT PCRs Entry: Disabled

3. Upload the trust chain certificates by navigating to the **Configuration** panel, then selecting **Trust Chain Management**.



Attestation Certificate Authority

Version: 2.0.2.1614975218.e045b8

Welcome to the HIRS Attestation CA

Configuration

Policy
Configure Identity CA and Supply Chain validation policies.

Trust Chain Management
Upload, view and manage CA certificates that complete trust chains for hardware credentials.

Platform Certificates
Upload, view and manage platform credentials.

Endorsement Certificates
Upload, view and manage endorsement credentials.

Reference Integrity Manifests
Upload, view and manage reference integrity manifests.

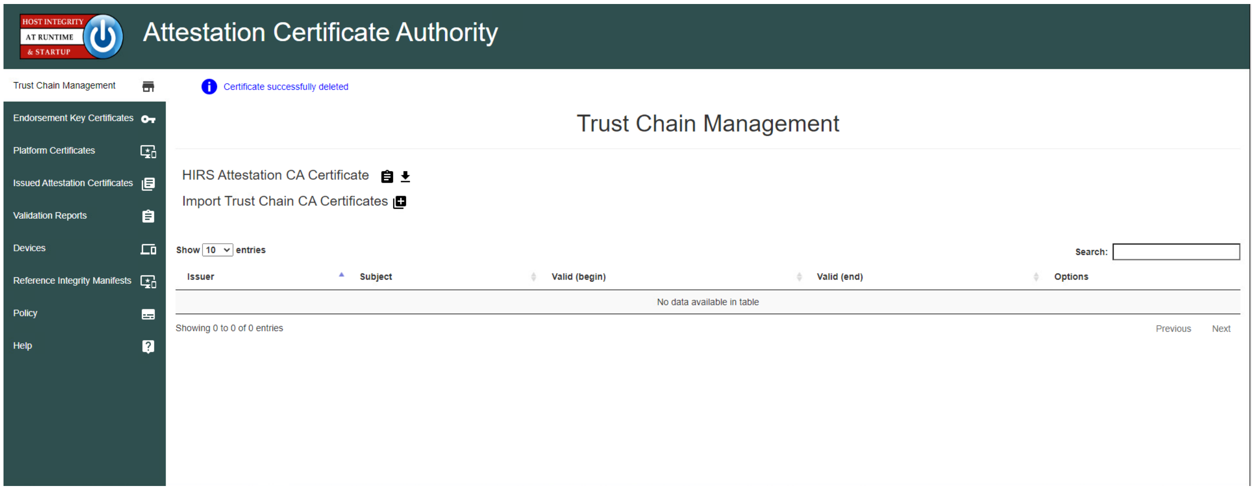
Status

Issued Attestation Certificates
View Attestation Certificates issued by this CA

Validation Reports
View a list of device validations carried out by this CA.

Devices
View devices covered by this CA for supply chain validation.

4. Select the icon beside **Import Trust Chain CA Certificates**.


HOST INTEGRITY AT RUNTIME & STARTUP
Attestation Certificate Authority
Trust Chain Management
Endorsement Key Certificates
Platform Certificates
Issued Attestation Certificates
Validation Reports
Devices
Reference Integrity Manifests
Policy
Help
Previous
Next

Certificate successfully deleted

Trust Chain Management

HIRS Attestation CA Certificate

Import Trust Chain CA Certificates

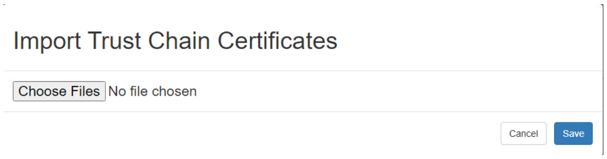
Show 10 entries

Search:

Issuer	Subject	Valid (begin)	Valid (end)	Options
No data available in table				

Showing 0 to 0 of 0 entries

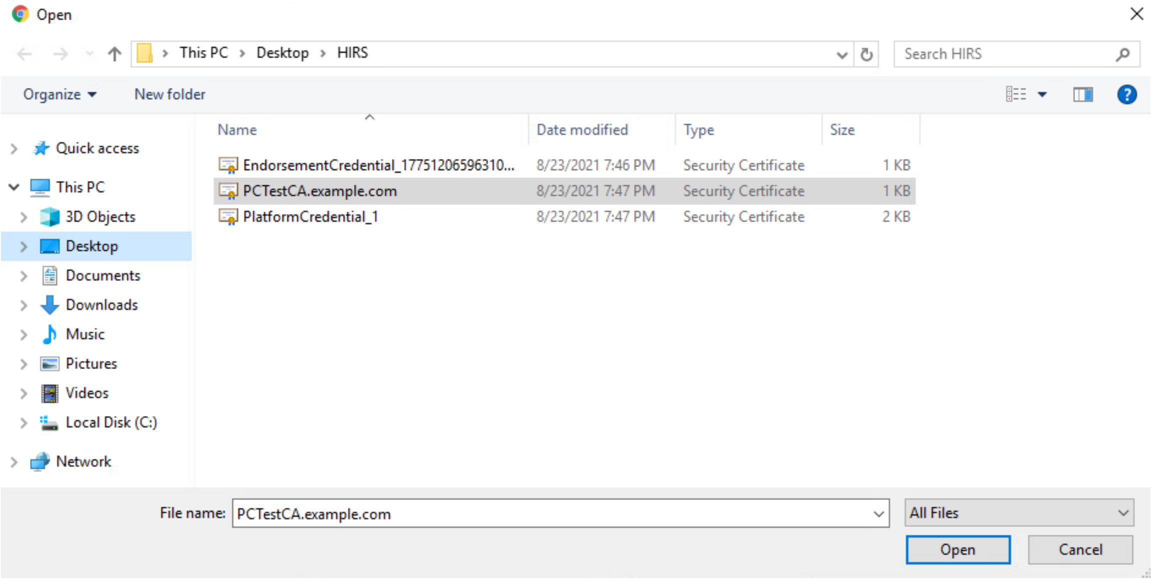
5. Select **Choose Files**.



Import Trust Chain Certificates

No file chosen

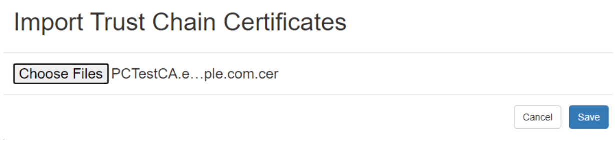
6. Select the Trust Chain Certificate from the local computer. For this project, the .crt file is ***PCTestCA.example.com***. Select the file and click **Open**.



Name	Date modified	Type	Size
EndorsementCredential_17751206596310...	8/23/2021 7:46 PM	Security Certificate	1 KB
PCTestCA.example.com	8/23/2021 7:47 PM	Security Certificate	1 KB
PlatformCredential_1	8/23/2021 7:47 PM	Security Certificate	2 KB

File name: PCTestCA.example.com

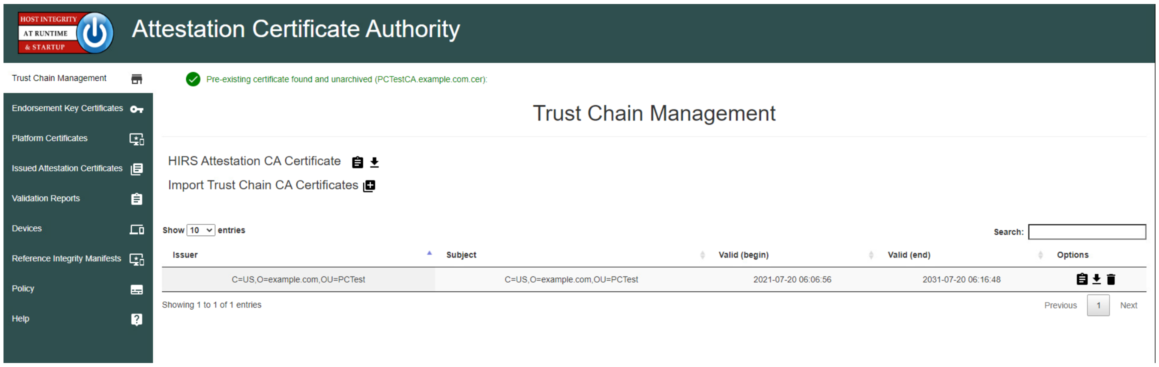
7. Select **Save.**



Import Trust Chain Certificates

Choose Files PCTestCA.e…ple.com.cer

8. The Trust Chain certificate should appear under the **Trust Chain Management** tab. Repeat this process for all root and intermediate certificates.



HOST INTEGRITY
AT RUNTIME
& STARTUP
Attestation Certificate Authority
Trust Chain Management
Endorsement Key Certificates
Platform Certificates
Issued Attestation Certificates
Validation Reports
Devices
Reference Integrity Manifests
Policy
Help

Pre-existing certificate found and unarchived (PCTestCA.example.com.cer):

Trust Chain Management

HIRS Attestation CA Certificate

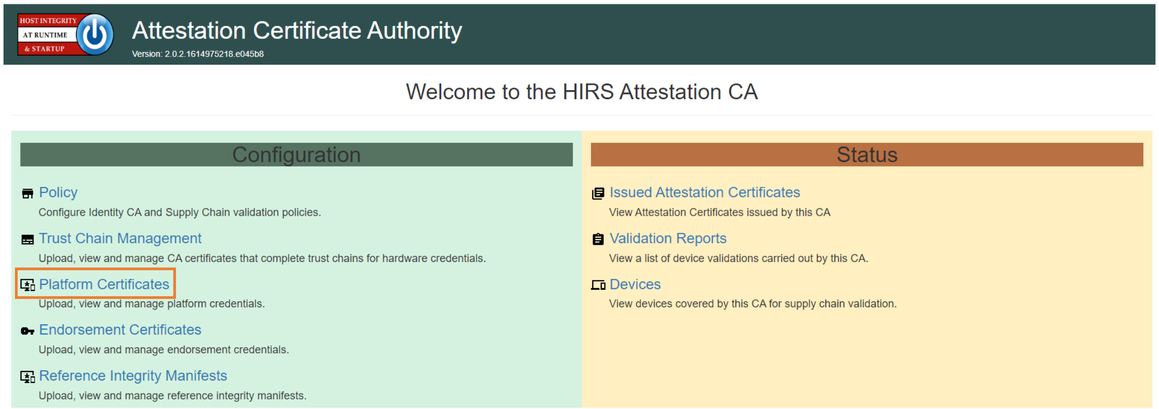
Import Trust Chain CA Certificates

Show 10 entries　　Search:

Issuer	Subject	Valid (begin)	Valid (end)	Options
C=US,O=example.com,OU=PCTest	C=US,O=example.com,OU=PCTest	2021-07-20 06:06:56	2031-07-20 06:16:48	

Showing 1 to 1 of 1 entries

9. Update the Platform Attribute certificates by navigating to the **Configurations** panel, then selecting **Platform Certificates**.



Version: 2.0.2.1614975218.e045b8

Welcome to the HIRS Attestation CA

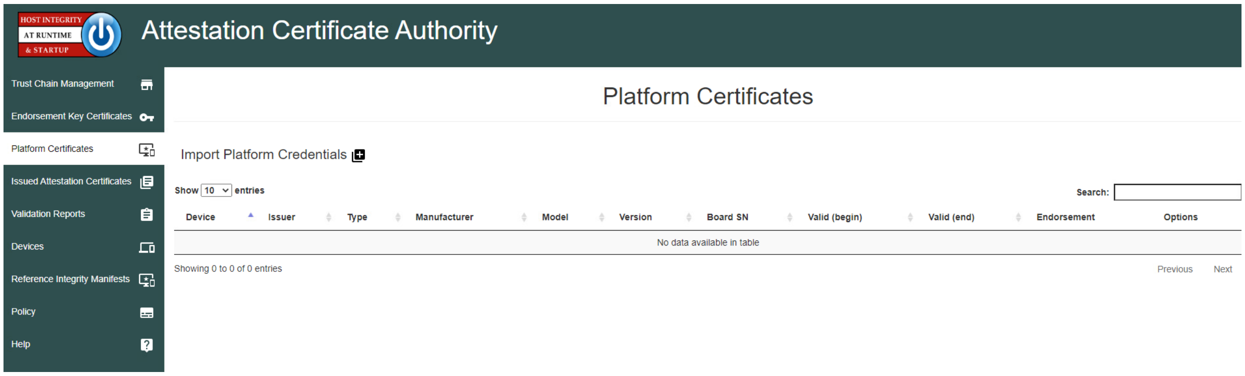
Configuration

- Policy
  Configure Identity CA and Supply Chain validation policies.
- Trust Chain Management
  Upload, view and manage CA certificates that complete trust chains for hardware credentials.
- Platform Certificates
  Upload, view and manage platform credentials.
- Endorsement Certificates
  Upload, view and manage endorsement credentials.
- Reference Integrity Manifests
  Upload, view and manage reference integrity manifests.

Status

- Issued Attestation Certificates
  View Attestation Certificates issued by this CA
- Validation Reports
  View a list of device validations carried out by this CA.
- Devices
  View devices covered by this CA for supply chain validation.

10. Select the icon beside Import Platform Certificates.



HOST INTEGRITY AT RUNTIME & STARTUP
Attestation Certificate Authority
Trust Chain Management
Endorsement Key Certificates
Platform Certificates
Issued Attestation Certificates
Validation Reports
Devices
Reference Integrity Manifests
Policy
Help

Platform Certificates

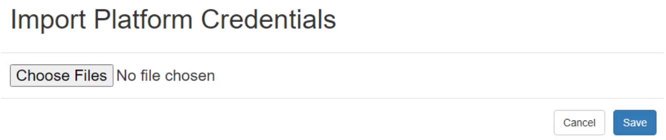
Import Platform Credentials

Show 10 entries Search:

Device	Issuer	Type	Manufacturer	Model	Version	Board SN	Valid (begin)	Valid (end)	Endorsement	Options
No data available in table										

Showing 0 to 0 of 0 entries

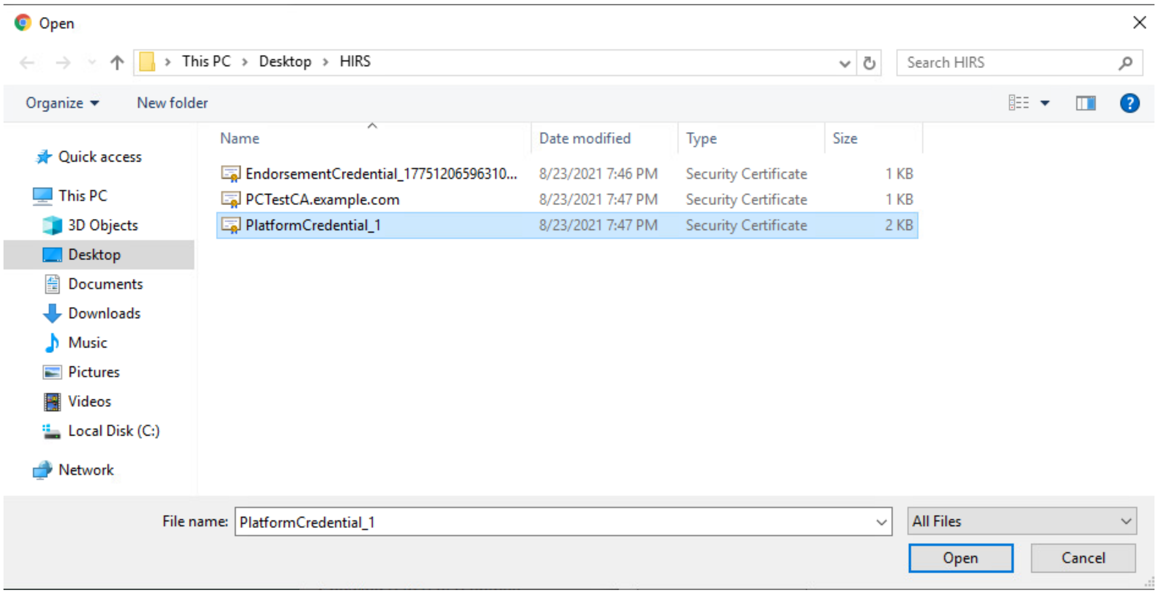
11. Select **Choose Files.**



Import Platform Credentials

No file chosen

12. Select the Platform Certificate from the local computer. For this project, the .crt file is **PlatformCredential_1**. Select the file and click **Open**.

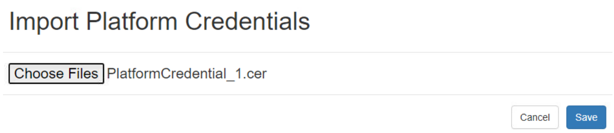


Name	Date modified	Type	Size
EndorsementCredential_17751206596310...	8/23/2021 7:46 PM	Security Certificate	1 KB
PCTestCA.example.com	8/23/2021 7:47 PM	Security Certificate	1 KB
PlatformCredential_1	8/23/2021 7:47 PM	Security Certificate	2 KB

File name: PlatformCredential_1

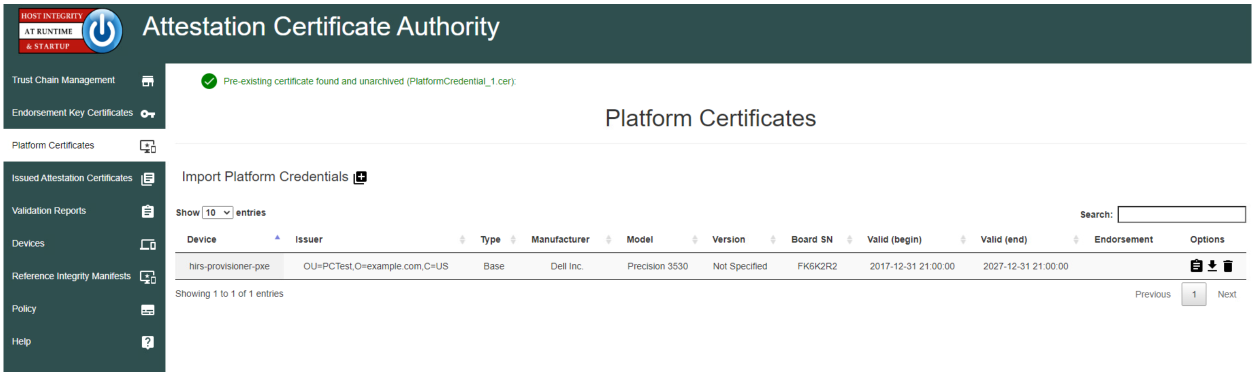
All Files

13. Select **Save**.



Import Platform Credentials

14. The Platform certificate should appear under the **Platform Certificates** tab.



Attestation Certificate Authority

Pre-existing certificate found and unarchived (PlatformCredential_1.cer):

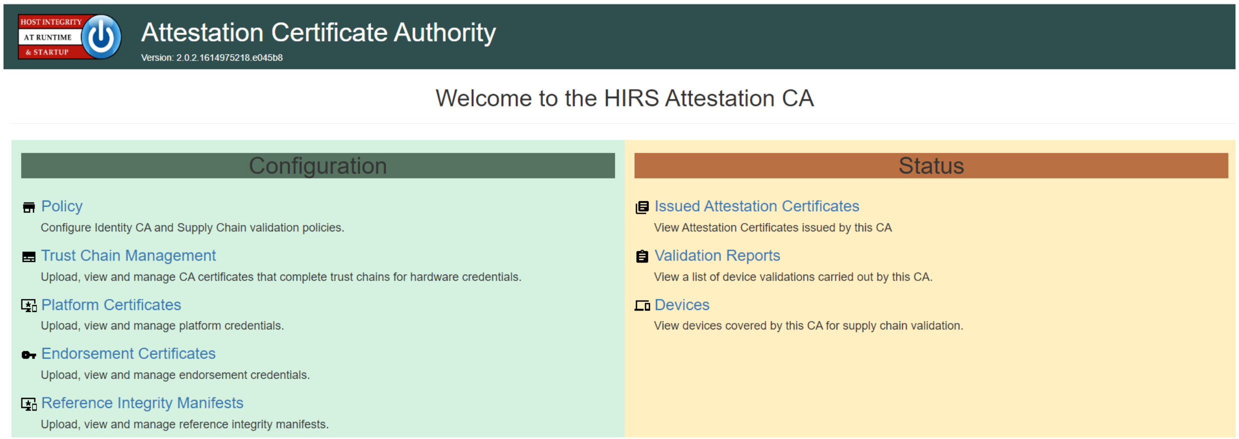
Platform Certificates

Show 10 entries | Search:

Device	Issuer	Type	Manufacturer	Model	Version	Board SN	Valid (begin)	Valid (end)	Endorsement	Options
hirs-provisioner-pxe	OU=PCTest,O=example.com,C=US	Base	Dell Inc.	Precision 3530	Not Specified	FK6K2R2	2017-12-31 21:00:00	2027-12-31 21:00:00		

Showing 1 to 1 of 1 entries

15. Upload the Endorsement Key certificate by navigating to the **Configuration** panel, then selecting **Endorsement Certificates**.



Attestation Certificate Authority

Version: 2.0.2.1614975218.e045b8

Welcome to the HIRS Attestation CA

Configuration

Policy
Configure Identity CA and Supply Chain validation policies.

Trust Chain Management
Upload, view and manage CA certificates that complete trust chains for hardware credentials.

Platform Certificates
Upload, view and manage platform credentials.

Endorsement Certificates
Upload, view and manage endorsement credentials.

Reference Integrity Manifests
Upload, view and manage reference integrity manifests.

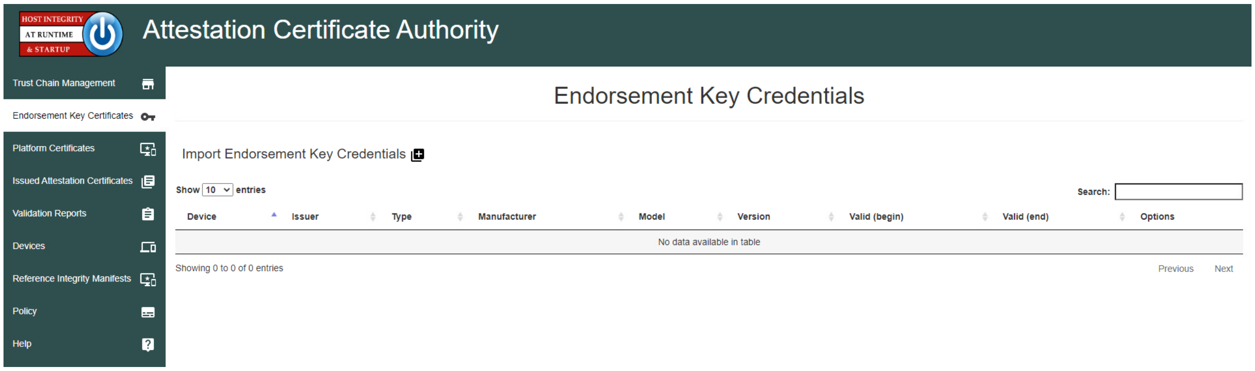
Status

Issued Attestation Certificates
View Attestation Certificates issued by this CA

Validation Reports
View a list of device validations carried out by this CA.

Devices
View devices covered by this CA for supply chain validation.

16. Select the icon beside **Import Endorsement Key Certificates**.


HOST INTEGRITY
AT RUNTIME
& STARTUP
Attestation Certificate Authority
Trust Chain Management
Endorsement Key Certificates
Platform Certificates
Issued Attestation Certificates
Validation Reports
Devices
Reference Integrity Manifests
Policy
Help

Endorsement Key Credentials

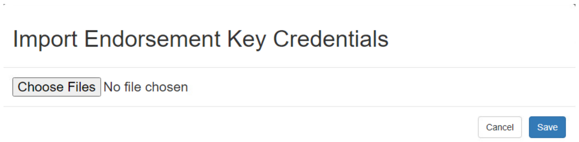
Import Endorsement Key Credentials

Show 10 entries Search:

Device	Issuer	Type	Manufacturer	Model	Version	Valid (begin)	Valid (end)	Options
No data available in table								

Showing 0 to 0 of 0 entries

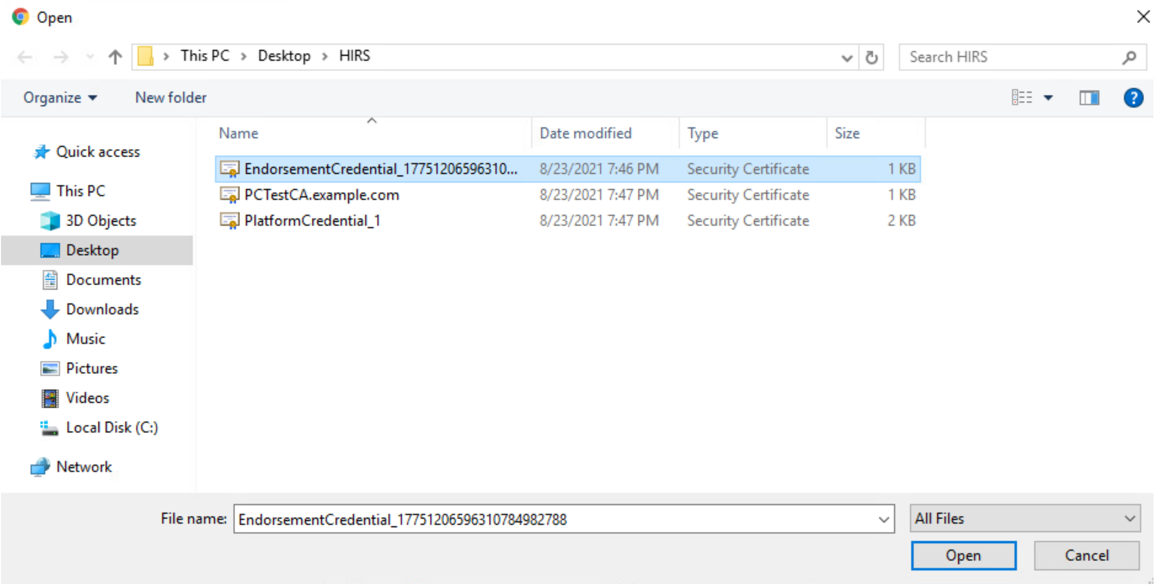
17. Select **Choose Files**.



Import Endorsement Key Credentials

Choose Files No file chosen

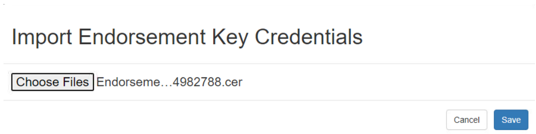
18. Select the Endorsement Credential from the local computer. For this project, the .crt file is *EndorsementCredential_17751206596310784982788*. Select the file and click **Open**.



Name	Date modified	Type	Size
EndorsementCredential_17751206596310...	8/23/2021 7:46 PM	Security Certificate	1 KB
PCTestCA.example.com	8/23/2021 7:47 PM	Security Certificate	1 KB
PlatformCredential_1	8/23/2021 7:47 PM	Security Certificate	2 KB

File name: EndorsementCredential_17751206596310784982788

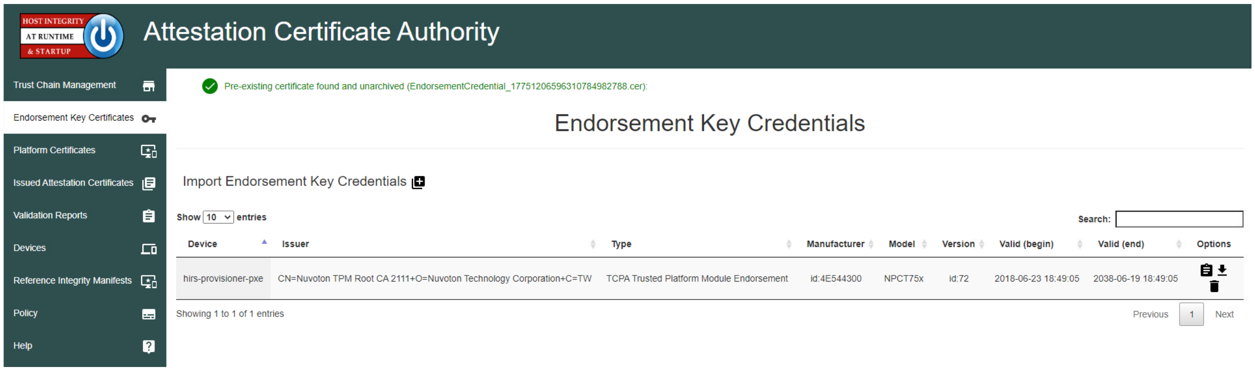
19. Select **Save.**



Import Endorsement Key Credentials

Choose Files Endorseme…4982788.cer

20. The Endorsement Key certificate should appear under the **Endorsement Key Credentials** tab.



HOST INTEGRITY
AT RUNTIME
& STARTUP
Attestation Certificate Authority
Trust Chain Management
Endorsement Key Certificates
Platform Certificates
Issued Attestation Certificates
Validation Reports
Devices
Reference Integrity Manifests
Policy
Help
Import Endorsement Key Credentials
Show 10 entries
Search:
Previous
1
Next

Pre-existing certificate found and unarchived (EndorsementCredential_177512065963107849827788.cer):

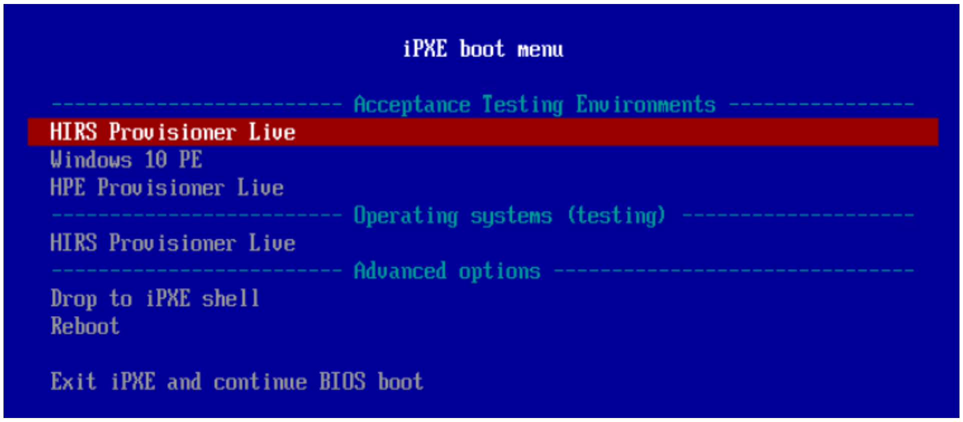
Endorsement Key Credentials

Device	Issuer	Type	Manufacturer	Model	Version	Valid (begin)	Valid (end)	Options
hirs-provisioner-pxe	CN=Nuvoton TPM Root CA 2111+O=Nuvoton Technology Corporation+C=TW	TCPA Trusted Platform Module Endorsement	id:4E544300	NPCT75x	id:72	2018-06-23 18:49:05	2038-06-19 18:49:05	

Showing 1 to 1 of 1 entries

3.1.1.2 Dell and HP Inc. Laptops

1. Boot the target laptop into the CentOS7 acceptance testing environment via iPXE. This typically requires a one-time boot execution to prevent the laptop from loading the native OS. Consult the manufacturer's documentation for the appropriate steps. Choose HIRS Provisioner Live from the iPXE boot menu.



```
                           iPXE boot menu

 ------------------------- Acceptance Testing Environments ----------------
 HIRS Provisioner Live
 Windows 10 PE
 HPE Provisioner Live
 ------------------------- Operating systems (testing) --------------------
 HIRS Provisioner Live
 ------------------------- Advanced options -------------------------------
 Drop to iPXE shell
 Reboot

 Exit iPXE and continue BIOS boot
```

2. Once the live environment has loaded, log in as a user with root privileges. Run the provision.sh script. The script will attempt to:
   - Change the hostname of the live environment. This assists the administrator in locating the target machine in the Eclypsium console.
   - Run the Eclypsium scanner and submit results to the Eclypsium Analytic cloud platform.
   - Run the HIRS provisioning script. If successful, post the results to the PMCS.

The script will exit at any point an error is detected. Refer to the comments in the script to set this up in your own environment. Up-to-date information related to debugging the HIRS provisioning process can be found on the project site.

3.1.1.2.1 HP Inc. installation of firmware event and configuration monitoring tools

This section is a work-in-progress and will be completed in a future iteration.

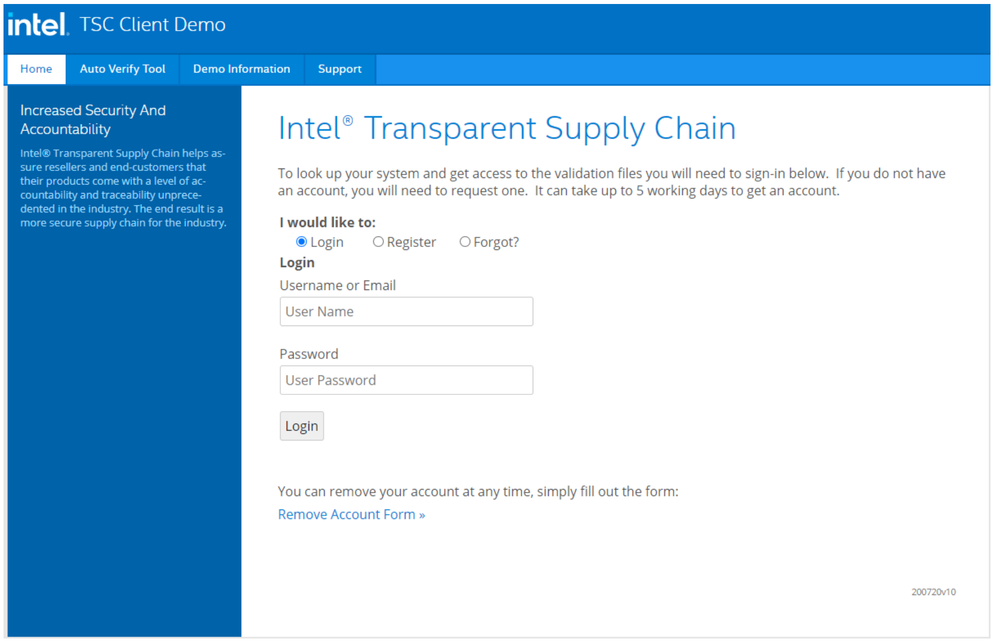
3.1.1.3 Intel-Contributed Laptops

The Auto Verify tool is central to scenario 2 acceptance testing. The tool compares the Direct Platform Data (DPD), allowing the customer to identify certain system changes from the time of manufacturing to the time of first boot. Install the Auto Verify Tool on the target system before attempting to execute the steps in this section.

The DPD files and platform certificate files for the target laptop are available from Intel's Transparent Supply Chain demo page, https://tsc.intel.com/client-demo/. Work with your Intel representative to obtain credentials for your organization.

3.1.1.3.1 Download DPD File and Platform Certificate

1. Authenticate to the Intel TSC Client Demo portal page.



Increased Security And Accountability

Intel® Transparent Supply Chain helps assure resellers and end-customers that their products come with a level of accountability and traceability unprecedented in the industry. The end result is a more secure supply chain for the industry.

Intel® Transparent Supply Chain

To look up your system and get access to the validation files you will need to sign-in below. If you do not have an account, you will need to request one. It can take up to 5 working days to get an account.

I would like to:

● Login ○ Register ○ Forgot?

Login

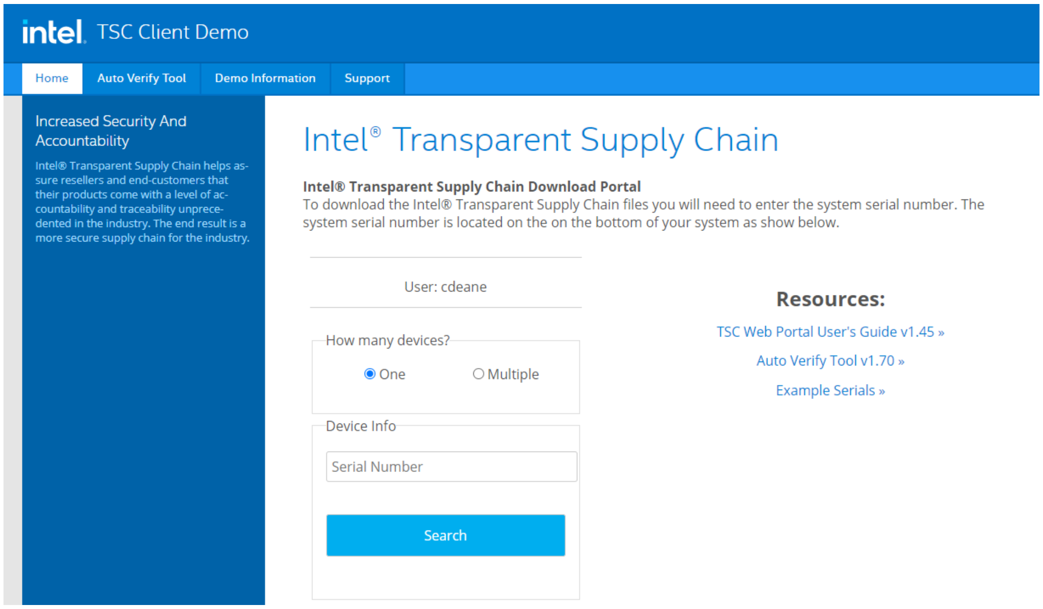
Username or Email: User Name

Password: User Password

You can remove your account at any time, simply fill out the form:
Remove Account Form »

200720v10

2. Enter the serial number of the Intel Laptop. Select **Search.**



Increased Security And Accountability

Intel® Transparent Supply Chain helps assure resellers and end-customers that their products come with a level of accountability and traceability unprecedented in the industry. The end result is a more secure supply chain for the industry.

Intel® Transparent Supply Chain

Intel® Transparent Supply Chain Download Portal
To download the Intel® Transparent Supply Chain files you will need to enter the system serial number. The system serial number is located on the on the bottom of your system as show below.

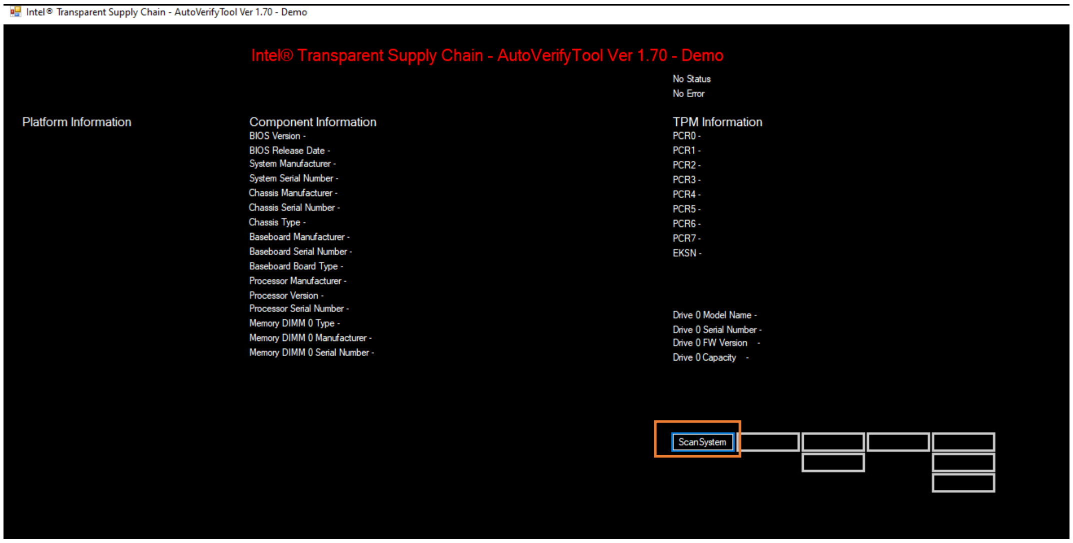
User: cdeane

How many devices?
● One ○ Multiple

Device Info
Serial Number

Resources:
TSC Web Portal User's Guide v1.45 »
Auto Verify Tool v1.70 »
Example Serials »

3. Download the zip file containing the DPD files and platform certificate. Save and unzip the file on the target laptop. These files will be used with the AutoVerify tool to determine if any components have been changed.
4. Launch the Auto Verify Tool.
5. Click the **Scan System** button.


Intel® Transparent Supply Chain - AutoVerifyTool Ver 1.70 - Demo

Intel® Transparent Supply Chain - AutoVerifyTool Ver 1.70 - Demo

No Status
No Error

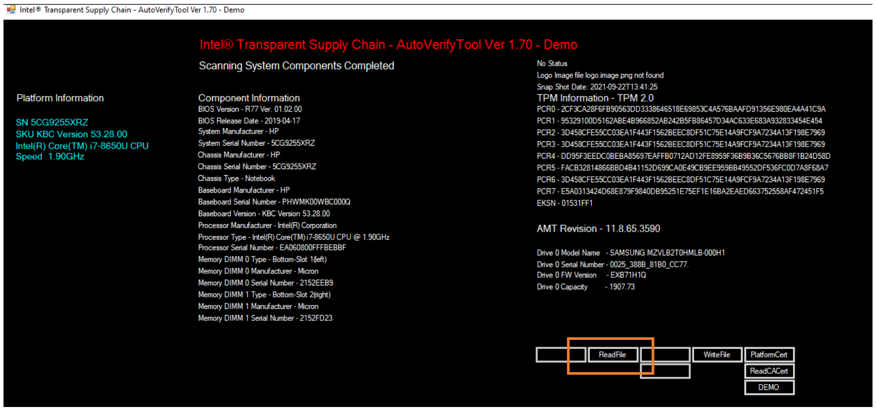
Platform Information

Component Information
BIOS Version -
BIOS Release Date -
System Manufacturer -
System Serial Number -
Chassis Manufacturer -
Chassis Serial Number -
Chassis Type -
Baseboard Manufacturer -
Baseboard Serial Number -
Baseboard Board Type -
Processor Manufacturer -
Processor Version -
Processor Serial Number -
Memory DIMM 0 Type -
Memory DIMM 0 Manufacturer -
Memory DIMM 0 Serial Number -

TPM Information
PCR0 -
PCR1 -
PCR2 -
PCR3 -
PCR4 -
PCR5 -
PCR6 -
PCR7 -
EKSN -

Drive 0 Model Name -
Drive 0 Serial Number -
Drive 0 FW Version -
Drive 0 Capacity -

6. The Auto Verify Tool should populate the Component Information entries with the platform details of the computer. To compare the data to the DPD file stored on the local computer, click **ReadFile**.



Intel® Transparent Supply Chain - AutoVerifyTool Ver 1.70 - Demo

Intel® Transparent Supply Chain - AutoVerifyTool Ver 1.70 - Demo

Scanning System Components Completed

Platform Information

SN 5CG9255XRZ
SKU KBC Version 53.28.00
Intel(R) Core(TM) i7-8650U CPU
Speed 1.90GHz

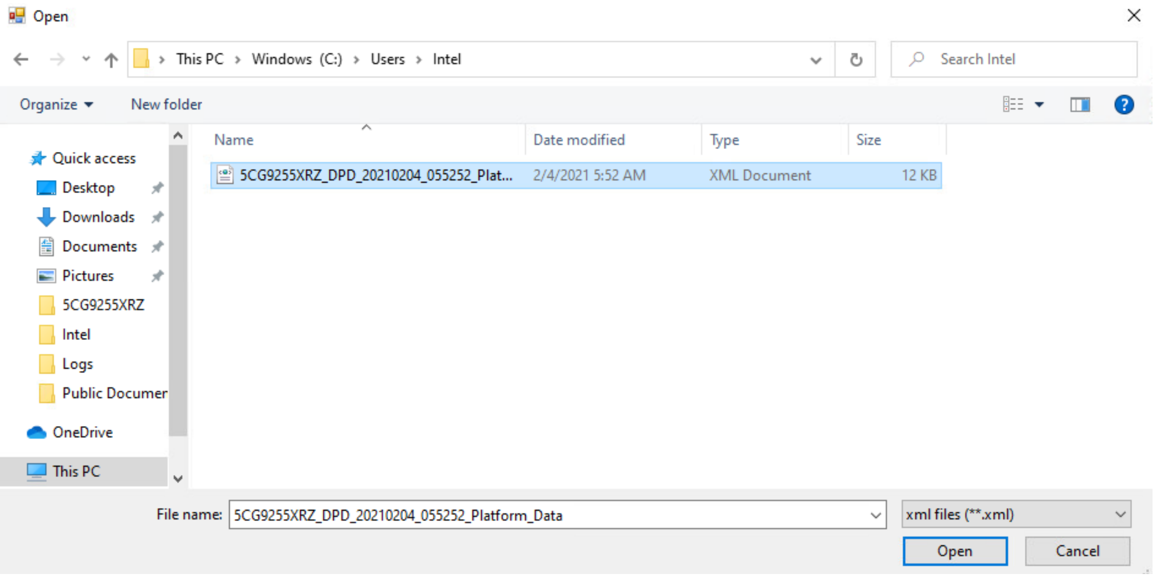
Component Information
BIOS Version - R77 Ver. 01.02.00
BIOS Release Date - 2019-04-17
System Manufacturer - HP
System Serial Number - 5CG9255XRZ
Chassis Manufacturer - HP
Chassis Serial Number - 5CG9255XRZ
Chassis Type - Notebook
Baseboard Manufacturer - HP
Baseboard Serial Number - PHWMK00WBC000Q
Baseboard Version - KBC Version 53.28.00
Processor Manufacturer - Intel(R) Corporation
Processor Type - Intel(R) Core(TM) i7-8650U CPU @ 1.90GHz
Processor Serial Number - EA060800FFFBEBBF
Memory DIMM 0 Type - Bottom-Slot 1(left)
Memory DIMM 0 Manufacturer - Micron
Memory DIMM 0 Serial Number - 2152EEB9
Memory DIMM 1 Type - Bottom-Slot 2(right)
Memory DIMM 1 Manufacturer - Micron
Memory DIMM 1 Serial Number - 2152FD23

No Status
Logo Image file logo.image.png not found
Snap Shot Date: 2021-09-22T13:41:25
TPM Information - TPM 2.0
PCR0 - 2CF3CA28F6FB90563DD3338646518E69853C4A576BAAFD91356E980EA4A41C9A
PCR1 - 95329100D5162ABE4B966852AB242B5FB86457D34AC633E683A932833454E454
PCR2 - 3D458CFE55CC03EA1F443F1562BEEC8DF51C75E14A9FCF9A7234A13F198E7969
PCR3 - 3D458CFE55CC03EA1F443F1562BEEC8DF51C75E14A9FCF9A7234A13F198E7969
PCR4 - DD95F3EEDC0BEBA85697EAFFB0712AD12FE8959F36B9B36C5676BB8F1B24D58D
PCR5 - FACB32814866BBD4B41152D699CA0E49CB9EE959BB49552DF536FC0D7A8F68A7
PCR6 - 3D458CFE55CC03EA1F443F1562BEEC8DF51C75E14A9FCF9A7234A13F198E7969
PCR7 - E5A0313424D68E879F9840DB95251E75EF1E16BA2EAED663752558AF472451F5
EKSN - 01531FF1

AMT Revision - 11.8.65.3590

Drive 0 Model Name - SAMSUNG MZVLB2T0HMLB-000H1
Drive 0 Serial Number - 0025_388B_81B0_CC77.
Drive 0 FW Version - EXB71H1Q
Drive 0 Capacity - 1907.73

7. Navigate to the downloaded DPD file and select **Open.**



Open

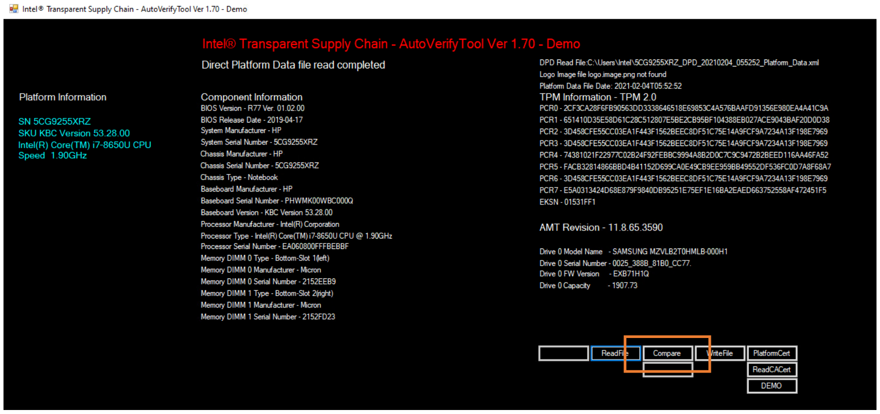
This PC › Windows (C:) › Users › Intel

Name	Date modified	Type	Size
5CG9255XRZ_DPD_20210204_055252_Plat...	2/4/2021 5:52 AM	XML Document	12 KB

File name: 5CG9255XRZ_DPD_20210204_055252_Platform_Data

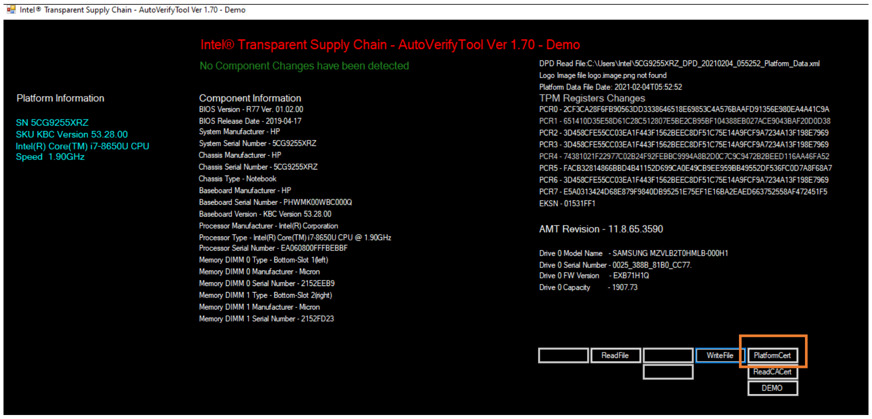
xml files (**.xml)

8. Next, click the **Compare** button.



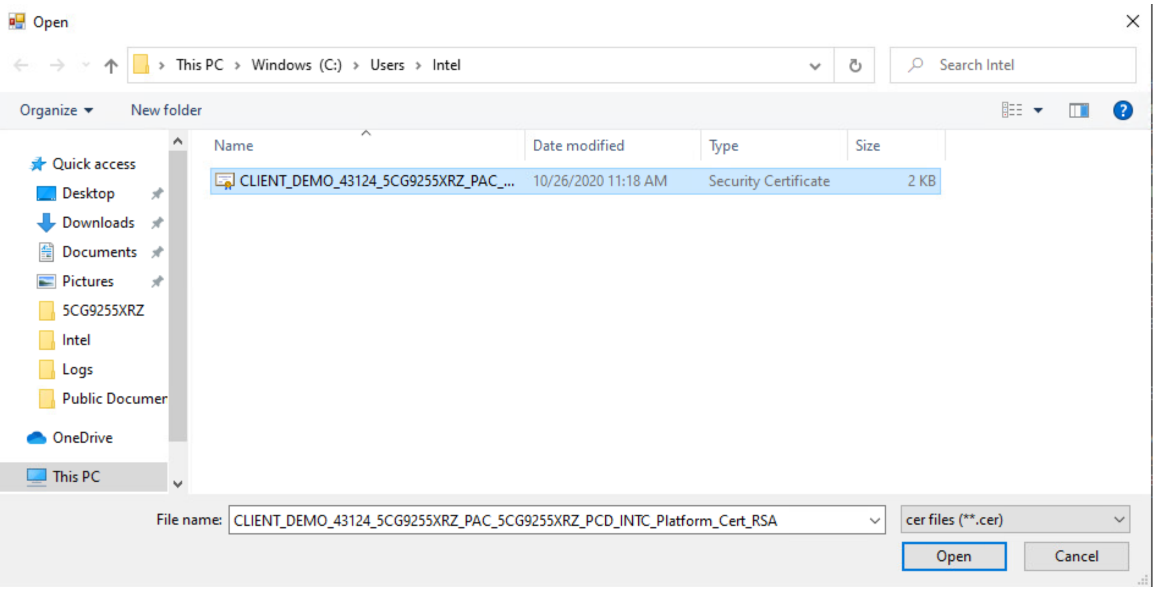
```
Intel® Transparent Supply Chain - AutoVerifyTool Ver 1.70 - Demo

Intel® Transparent Supply Chain - AutoVerifyTool Ver 1.70 - Demo
Direct Platform Data file read completed

Platform Information

SN 5CG9255XRZ
SKU KBC Version 53.28.00
Intel(R) Core(TM) i7-8650U CPU
Speed  1.90GHz

Component Information
BIOS Version - R77 Ver. 01.02.00
BIOS Release Date - 2019-04-17
System Manufacturer - HP
System Serial Number - 5CG9255XRZ
Chassis Manufacturer - HP
Chassis Serial Number - 5CG9255XRZ
Chassis Type - Notebook
Baseboard Manufacturer - HP
Baseboard Serial Number - PHWMK00WBC000Q
Baseboard Version - KBC Version 53.28.00
Processor Manufacturer - Intel(R) Corporation
Processor Type - Intel(R) Core(TM) i7-8650U CPU @ 1.90GHz
Processor Serial Number - EA060800FFFBEBBF
Memory DIMM 0 Type - Bottom-Slot 1(left)
Memory DIMM 0 Manufacturer - Micron
Memory DIMM 0 Serial Number - 2152EEB9
Memory DIMM 1 Type - Bottom-Slot 2(right)
Memory DIMM 1 Manufacturer - Micron
Memory DIMM 1 Serial Number - 2152FD23

DPD Read File:C:\Users\Intel\5CG9255XRZ_DPD_20210204_055252_Platform_Data.xml
Logo Image file logo.image.png not found
Platform Data File Date: 2021-02-04T05:52:52
TPM Information - TPM 2.0
PCR0 - 2CF3CA28F6FB90563DD3338646518E69853C4A576BAAFD91356E980EA4A41C9A
PCR1 - 651410D35E58D61C28C512807E5BE2CB95BF104388EB027ACE9043BAF20D0D38
PCR2 - 3D458CFE55CC03EA1F443F1562BEEC8DF51C75E14A9FCF9A7234A13F198E7969
PCR3 - 3D458CFE55CC03EA1F443F1562BEEC8DF51C75E14A9FCF9A7234A13F198E7969
PCR4 - 74381021F22977C02B24F92FEBBC9994A8B2D0C7C9C9472B2BEED116AA46FA52
PCR5 - FACB32814866BBD4B41152D699CA0E49CB9EE959BB49552DF536FC0D7A8F68A7
PCR6 - 3D458CFE55CC03EA1F443F1562BEEC8DF51C75E14A9FCF9A7234A13F198E7969
PCR7 - E5A0313424D68E879F9840DB95251E75EF1E16BA2EAED663752558AF472451F5
EKSN - 01531FF1

AMT Revision - 11.8.65.3590

Drive 0 Model Name   - SAMSUNG MZVLB2T0HMLB-000H1
Drive 0 Serial Number - 0025_388B_81B0_CC77.
Drive 0 FW Version    - EXB71H1Q
Drive 0 Capacity      - 1907.73
```

9. If no changes have been made, the Auto Verify tool should output a green message that says, "**No Component Changes have been detected**." To compare the certificate file, click the **PlatformCert** button.



```
Intel® Transparent Supply Chain - AutoVerifyTool Ver 1.70 - Demo

Intel® Transparent Supply Chain - AutoVerifyTool Ver 1.70 - Demo
No Component Changes have been detected

Platform Information

SN 5CG9255XRZ
SKU KBC Version 53.28.00
Intel(R) Core(TM) i7-8650U CPU
Speed  1.90GHz

Component Information
BIOS Version - R77 Ver. 01.02.00
BIOS Release Date - 2019-04-17
System Manufacturer - HP
System Serial Number - 5CG9255XRZ
Chassis Manufacturer - HP
Chassis Serial Number - 5CG9255XRZ
Chassis Type - Notebook
Baseboard Manufacturer - HP
Baseboard Serial Number - PHWMK00WBC000Q
Baseboard Version - KBC Version 53.28.00
Processor Manufacturer - Intel(R) Corporation
Processor Type - Intel(R) Core(TM) i7-8650U CPU @ 1.90GHz
Processor Serial Number - EA060800FFFBEBBF
Memory DIMM 0 Type - Bottom-Slot 1(left)
Memory DIMM 0 Manufacturer - Micron
Memory DIMM 0 Serial Number - 2152EEB9
Memory DIMM 1 Type - Bottom-Slot 2(right)
Memory DIMM 1 Manufacturer - Micron
Memory DIMM 1 Serial Number - 2152FD23

DPD Read File:C:\Users\Intel\5CG9255XRZ_DPD_20210204_055252_Platform_Data.xml
Logo Image file logo.image.png not found
Platform Data File Date: 2021-02-04T05:52:52
TPM Registers Changes
PCR0 - 2CF3CA28F6FB90563DD3338646518E69853C4A576BAAFD91356E980EA4A41C9A
PCR1 - 651410D35E58D61C28C512807E5BE2CB95BF104388EB027ACE9043BAF20D0D38
PCR2 - 3D458CFE55CC03EA1F443F1562BEEC8DF51C75E14A9FCF9A7234A13F198E7969
PCR3 - 3D458CFE55CC03EA1F443F1562BEEC8DF51C75E14A9FCF9A7234A13F198E7969
PCR4 - 74381021F22977C02B24F92FEBBC9994A8B2D0C7C9C9472B2BEED116AA46FA52
PCR5 - FACB32814866BBD4B41152D699CA0E49CB9EE959BB49552DF536FC0D7A8F68A7
PCR6 - 3D458CFE55CC03EA1F443F1562BEEC8DF51C75E14A9FCF9A7234A13F198E7969
PCR7 - E5A0313424D68E879F9840DB95251E75EF1E16BA2EAED663752558AF472451F5
EKSN - 01531FF1

AMT Revision - 11.8.65.3590

Drive 0 Model Name   - SAMSUNG MZVLB2T0HMLB-000H1
Drive 0 Serial Number - 0025_388B_81B0_CC77.
Drive 0 FW Version    - EXB71H1Q
Drive 0 Capacity      - 1907.73
```

10. Navigate to the location of the platform certificate and select **Open.**



Name	Date modified	Type	Size
CLIENT_DEMO_43124_5CG9255XRZ_PAC_...	10/26/2020 11:18 AM	Security Certificate	2 KB

File name: CLIENT_DEMO_43124_5CG9255XRZ_PAC_5CG9255XRZ_PCD_INTC_Platform_Cert_RSA

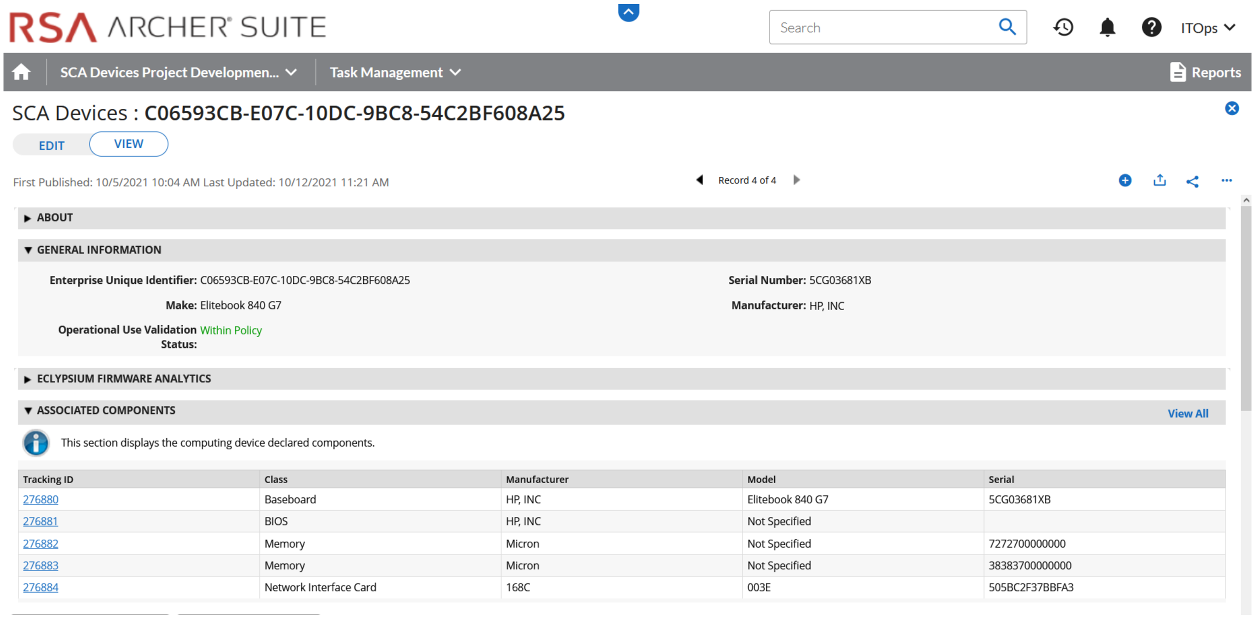
cer files (**.cer)

11. If the certificate matches the certificate that the AutoVerify tool detected, the tool will output another green message that says “**Platform Certificate Matches**.”

3.1.2 Asset Inventory and Discovery

Figure 3-1 shows a representative laptop computing device that has completed the acceptance testing process by an IT administrator. In the General Information section, we have opted to display characteristics that are common across all the manufacturers in our project such as the serial number and the make of the computing device. Separately in the Associated Components section, we store and track the components from the initial manufacturer manifest. We will continue to iterate on the asset inventory user interface to surface meaningful and easily understandable information that is appropriate for individuals responsible for IT security.

Figure 3-1 Asset Inventory Screenshot



SCA Devices : **C06593CB-E07C-10DC-9BC8-54C2BF608A25**

First Published: 10/5/2021 10:04 AM Last Updated: 10/12/2021 11:21 AM

▶ ABOUT

▼ GENERAL INFORMATION

Enterprise Unique Identifier: C06593CB-E07C-10DC-9BC8-54C2BF608A25

Serial Number: 5CG03681XB

Make: Elitebook 840 G7

Manufacturer: HP, INC

Operational Use Validation Status: Within Policy

▶ ECLYPSIUM FIRMWARE ANALYTICS

▼ ASSOCIATED COMPONENTS

This section displays the computing device declared components.

Tracking ID	Class	Manufacturer	Model	Serial
276880	Baseboard	HP, INC	Elitebook 840 G7	5CG03681XB
276881	BIOS	HP, INC	Not Specified	
276882	Memory	Micron	Not Specified	7272700000000
276883	Memory	Micron	Not Specified	38383700000000
276884	Network Interface Card	168C	003E	505BC2F37BBFA3

3.2 Scenario 3: Verification of Components During Use

In this scenario, the computing device has been accepted by the organization (Scenario 2) and has been provisioned for the end user. The computing device components are verified against the attributes and measurements declared by the manufacturer or purchasing organization during operational usage.

The general execution steps are as follows:

1. The end user takes ownership of the computing device from the IT department and uses it to perform daily work tasks within the scope of normal duties.

2. The computing device creates a report that attests to the platform attributes, such as device identity, hardware components, and firmware measurements that can be identified by interrogating the platform.

3. The attestation is consumed and validated by existing configuration management systems used by the IT organization as part of a continuous monitoring program.

4. The measured state of the device is maintained and updated as the authorized components of the device are being maintained and associated firmware is updated throughout the device's operational life cycle.

5. Optionally, the IT administrator takes a remediation action against the computing device if it is deemed out of compliance. For example, the computing device could be restricted from accessing certain corporate network resources.

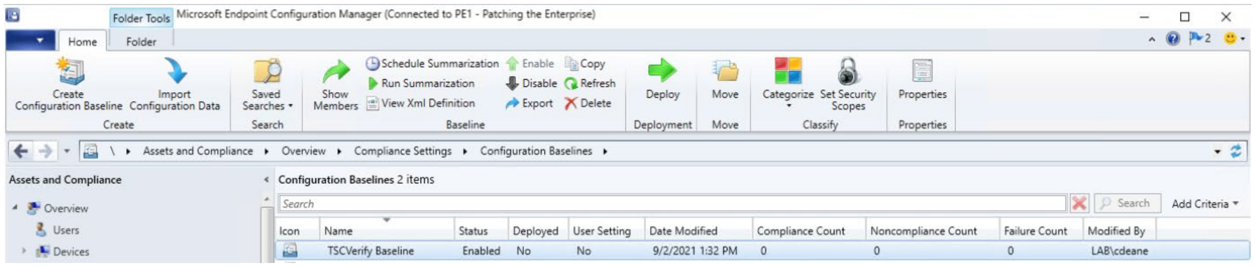
3.2.1 Technology Configurations

3.2.1.1 Intel TSC Monitoring

This section describes the steps that monitor for unexpected component changes using Intel TSC tooling and Microsoft Configuration Manager capabilities.

3.2.1.1.1 Deploy Baseline

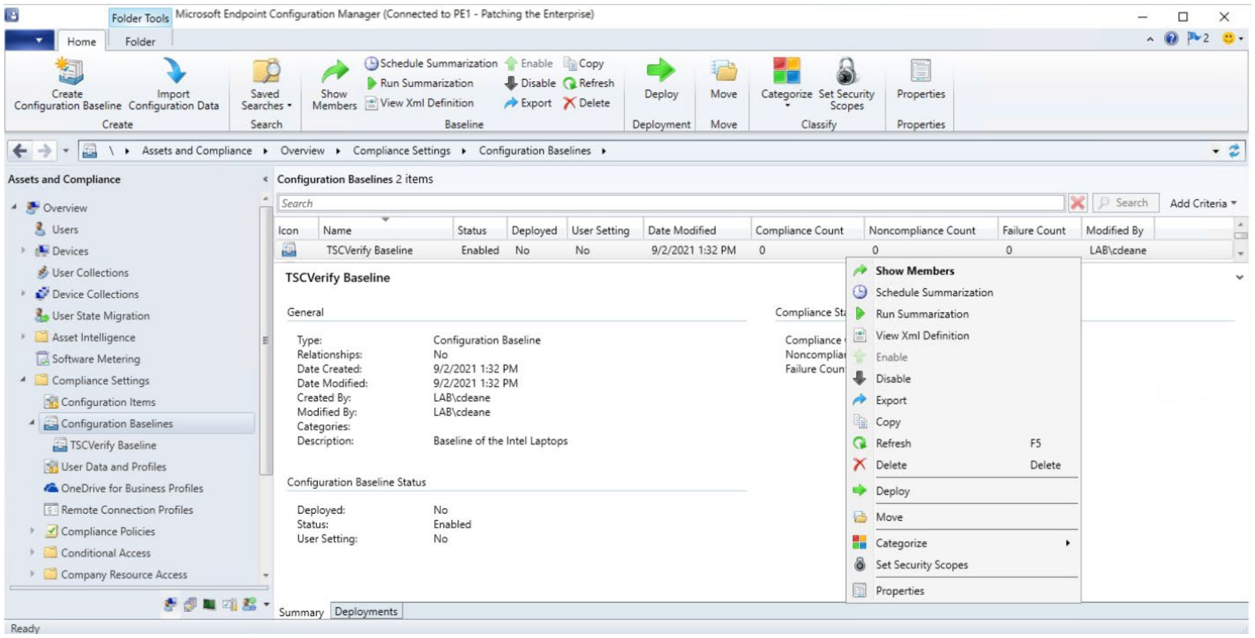
1. Navigate to the newly created configuration baseline located at **Assets and Compliance > Overview > Compliance Settings > Configuration Baselines.**



Configuration Baselines 2 items

Icon	Name	Status	Deployed	User Setting	Date Modified	Compliance Count	Noncompliance Count	Failure Count	Modified By
	TSCVerify Baseline	Enabled	No	No	9/2/2021 1:32 PM	0	0	0	LAB\cdeane

2. Right-click on the configuration baseline and select **Deploy.**



Configuration Baselines 2 items

Icon	Name	Status	Deployed	User Setting	Date Modified	Compliance Count	Noncompliance Count	Failure Count	Modified By
	TSCVerify Baseline	Enabled	No	No	9/2/2021 1:32 PM	0	0	0	LAB\cdeane

TSCVerify Baseline

General

Type: Configuration Baseline
Relationships: No
Date Created: 9/2/2021 1:32 PM
Date Modified: 9/2/2021 1:32 PM
Created By: LAB\cdeane
Modified By: LAB\cdeane
Categories:
Description: Baseline of the Intel Laptops

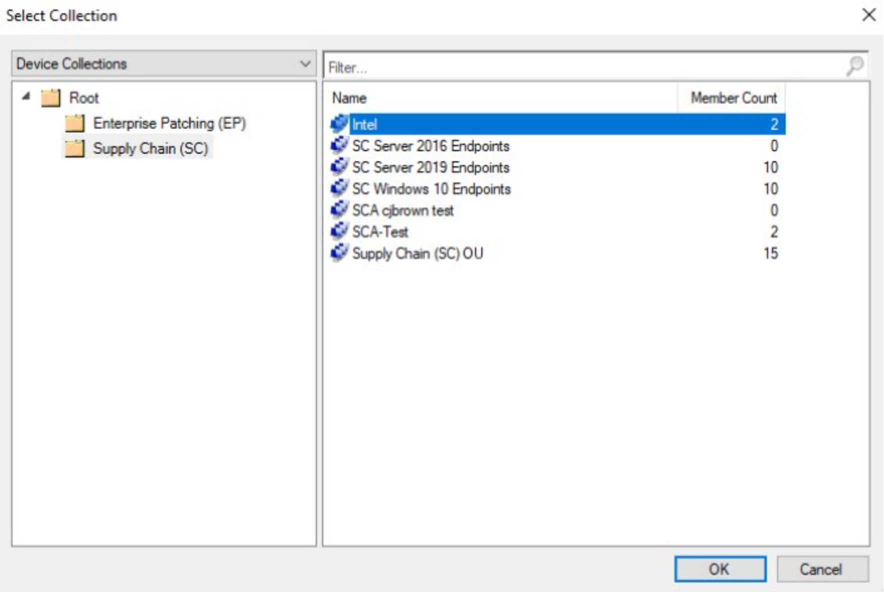
Compliance St

Compliance
Noncomplia
Failure Coun

Configuration Baseline Status

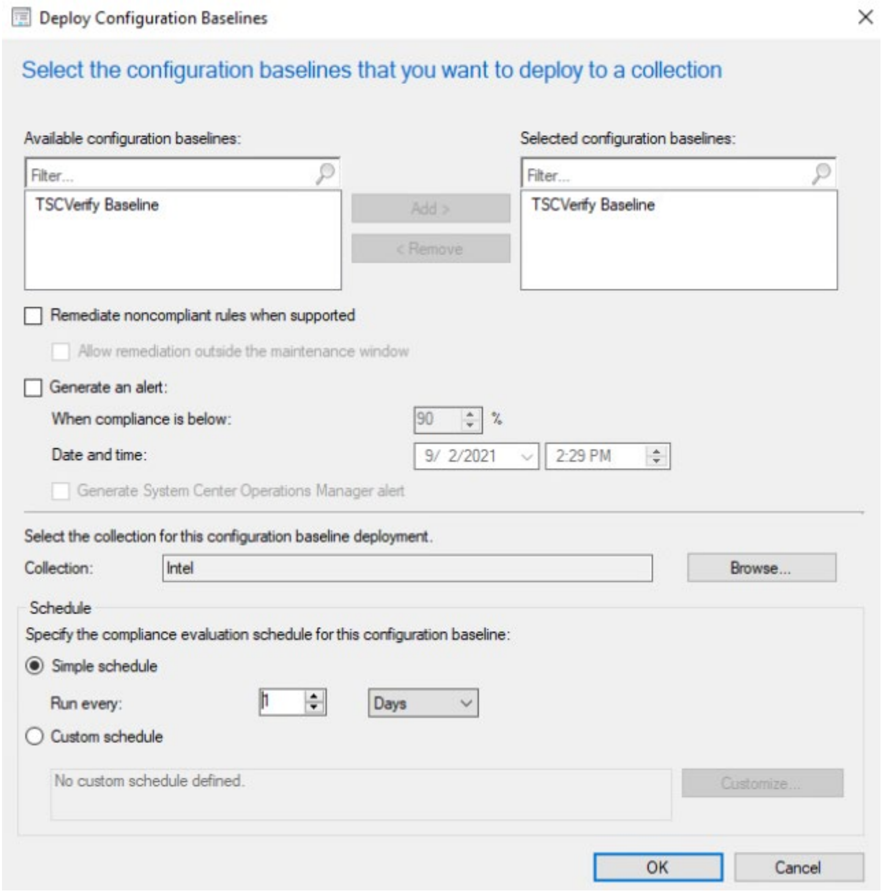
Deployed: No
Status: Enabled
User Setting: No

3. Select the device collection for the Intel TSC-supported machines. For this project, the device collection is called **Intel**. Select **OK**.



Name	Member Count
Intel	2
SC Server 2016 Endpoints	0
SC Server 2019 Endpoints	10
SC Windows 10 Endpoints	10
SCA cjbrown test	0
SCA-Test	2
Supply Chain (SC) OU	15

4. Ensure that the baseline is selected and then select the desired frequency of when to run the baseline. Select **OK**.



Deploy Configuration Baselines

Select the configuration baselines that you want to deploy to a collection

Available configuration baselines:

TSCVerify Baseline

Selected configuration baselines:

TSCVerify Baseline

□ Remediate noncompliant rules when supported

□ Allow remediation outside the maintenance window

□ Generate an alert:

When compliance is below: 90 %

Date and time: 9/ 2/2021 2:29 PM

□ Generate System Center Operations Manager alert

Select the collection for this configuration baseline deployment.

Collection: Intel

Schedule

Specify the compliance evaluation schedule for this configuration baseline:

● Simple schedule

Run every: 1 Days

○ Custom schedule

No custom schedule defined.

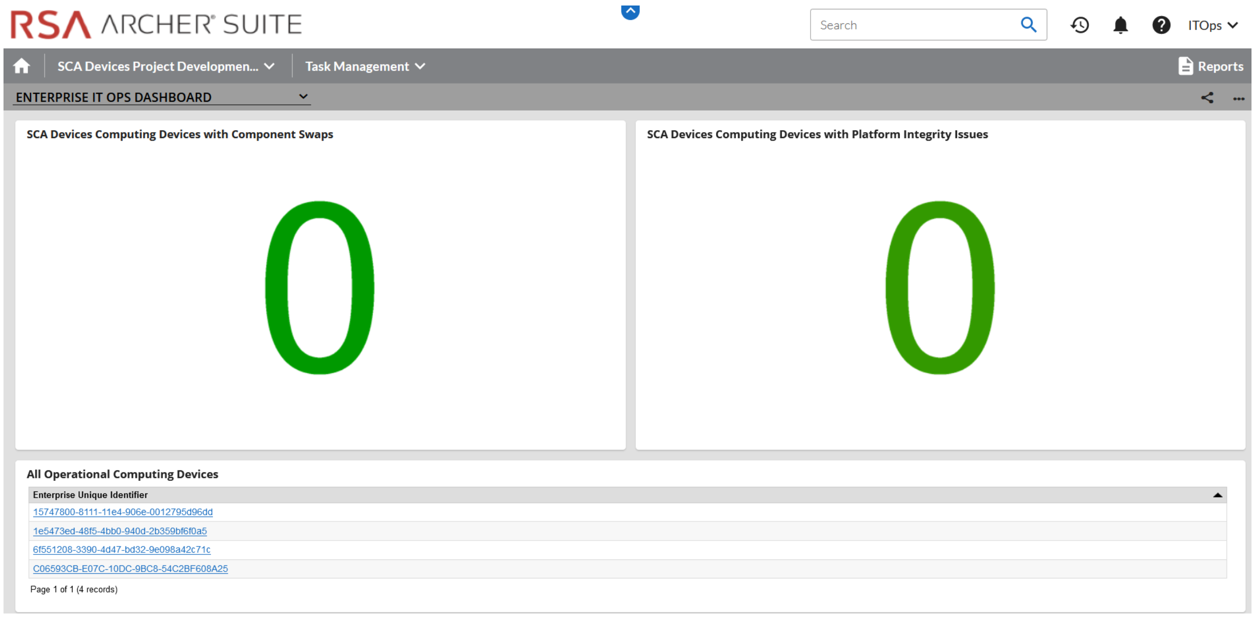
3.2.1.2 HP Inc. Firmware Integrity Monitoring

This section is a work-in-progress and will be completed in a future iteration.

3.2.2 Dashboards

The dashboard created in Section 2.10.2.3 attempts to consolidate and communicate potential integrity issues to the IT administrator while computing devices are in operational use. The timeliness of this information will depend on the cadence that your organization chooses to update the various data feeds from Microsoft Configuration Manager and the Eclypsium Analytic platform. This preliminary demonstration displays to the administrator if there are detected component swaps from computing devices that can leverage Intel TSC processes. Further, it displays any detected firmware platform integrity issues from the Eclypsium Analytic cloud platform across all manufacturers in this prototype. The RSA Archer dashboard should resemble the screenshots below, where a count of computing devices with potential integrity issues is displayed (Figure 3-2 and Figure 3-3). IT administrators may also want to access the Eclypsium Analytic platform directly to obtain detailed information, including remediation actions, for computing devices with detected integrity issues.

Figure 3-2 Dashboard with No Integrity Issues Detected


RSA ARCHER® SUITE
Search
ITOps
SCA Devices Project Developmen...
Task Management
Reports
ENTERPRISE IT OPS DASHBOARD

SCA Devices Computing Devices with Component Swaps

0

SCA Devices Computing Devices with Platform Integrity Issues

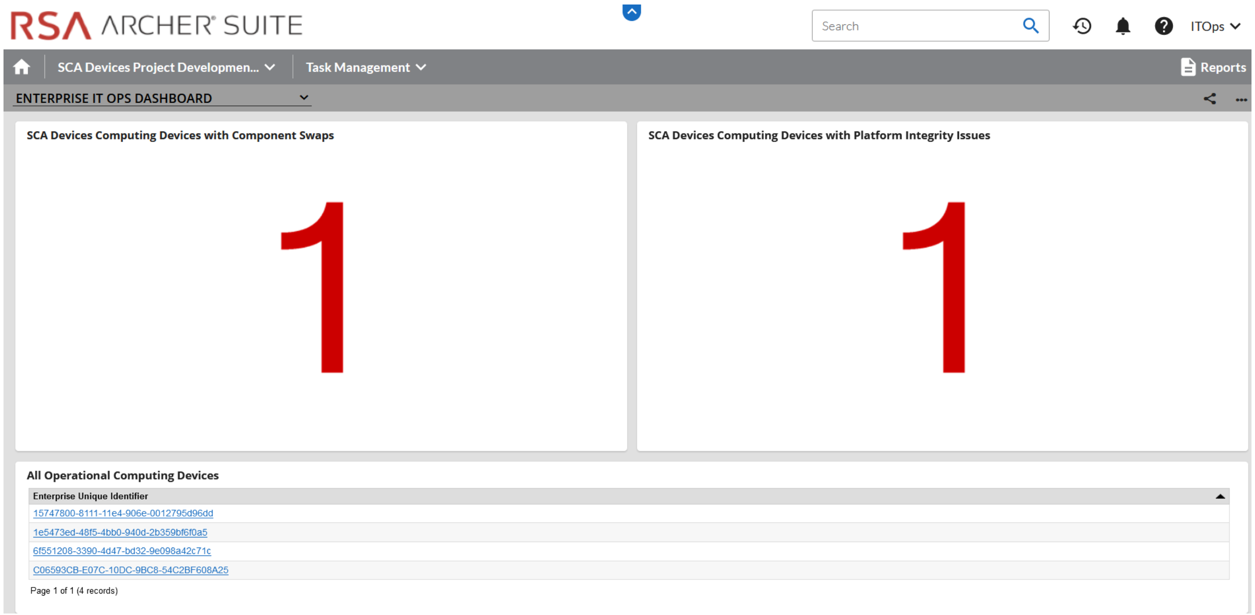
0

All Operational Computing Devices

Enterprise Unique Identifier
15747800-8111-11e4-906e-0012795d96dd
1e5473ed-48f5-4bb0-940d-2b359bf6f0a5
6f551208-3390-4d47-bd32-9e098a42c71c
C06593CB-E07C-10DC-9BC8-54C2BF608A25

Page 1 of 1 (4 records)

Figure 3-3 Dashboard with Integrity Issues Detected


RSA ARCHER® SUITE
Search
ITOps
SCA Devices Project Developmen...
Task Management
Reports
ENTERPRISE IT OPS DASHBOARD

SCA Devices Computing Devices with Component Swaps

1

SCA Devices Computing Devices with Platform Integrity Issues

1

All Operational Computing Devices

Enterprise Unique Identifier
15747800-8111-11e4-906e-0012795d96dd
1e5473ed-48f5-4bb0-940d-2b359bf6f0a5
6f551208-3390-4d47-bd32-9e098a42c71c
C06593CB-E07C-10DC-9BC8-54C2BF608A25

Page 1 of 1 (4 records)

Appendix A List of Acronyms

ACA	Attestation Certificate Authority
AD	Active Directory
ADK	(Windows) Assessment and Deployment Kit
API	Application Programming Interface
BIOS	Basic Input/Output System
CMSL	(HP) Client Management Script Library
DHCP	Dynamic Host Configuration Protocol
DPD	Direct Platform Data
DNS	Domain Name System
FQDN	Fully Qualified Domain Name
HIRS	Host Integrity at Runtime and Start-Up
HPE	Hewlett Packard Enterprise
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IIS	(Microsoft) Internet Information Services
IP	Internet Protocol
IT	Information Technology
NIST	National Institute of Standards and Technology
NCCoE	National Cybersecurity Center of Excellence
OEM	Original Equipment Manufacturer
OS	Operating System
PC	Personal Computer
PM2	Process Manager 2
PMCS	Platform Manifest Correlation System
PXE	Preboot Execution Environment

REST	Representational State Transfer
SCA	Supply Chain Assurance
SCRM	Supply Chain Risk Management
SP	Special Publication
SSMS	(Microsoft) SQL Server Management Studio
TEI	Trusted Enterprise Infrastructure
TFTP	Trivial File Transfer Protocol
TPM	Trusted Platform Module
TSC	(Intel) Transparent Supply Chain
UEFI	Unified Extensible Firmware Interface
UI	User Interface
URL	Uniform Resource Locator
XML	Extensible Markup Language