Honeywell | SYSTEM HINTS NEWSLETTER

HONEYWELL INFORMATION, NEWS, AND TIPS

In This Issue

Contents

Subscribe to HINTS

Login to www.HoneywellProcess.com. Go to Support > **Search Knowledge Base** and click on System HINTS under Latest Newsletters. In the page that opens, click on Subscribe to Support Newsletters (System HINTS)

The Search Knowledge Base page allows you to search our Knowledge Base with many technical support-related articles. So, if you need technical assistance, try the Knowledge Base first!
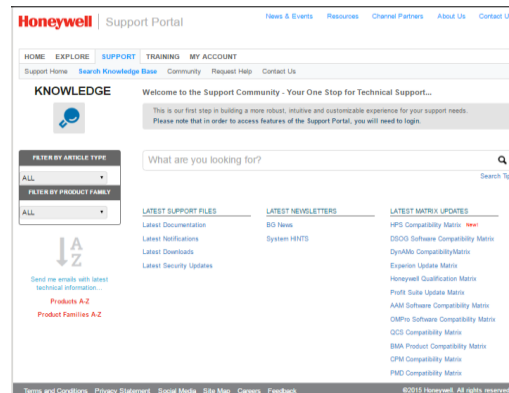
More Support Online (login)

You can also create a Support Request online. Monitor your Support Request cases by visiting the Request Help page. For all other support queries, please contact our Customer Contact Center.

For questions or comments related to the HINTS newsletter, please write to HPS System HINTS.

VTECH2020 you can still [register and participate](#)!

The live sessions have ended yet the platform is still open up till and including July 3, 2020.

Join the first Virtual Honeywell Process Solutions Conference: **Honeywell Virtual Technology Experience 2020**

You can use this platform to view all on demand sessions and breakout materials and visit our virtual Technology Expo.

From there you can go to your favorite topics, the virtual platform is available to you – yet without any live events up till July 3.

We look forward to your participation.

If you have any questions, feel free to reach out to usersgroup@honeywell.com

Experion Gold Standard System

Honeywell provides comprehensive documentation and support tools to assist customers with installing and maintaining Experion PKS. These resources contain configuration guidance, best practices, and links to the latest Experion and third-party updates that provide for a highly reliable, up to date Experion PKS environment.

An Experion Gold Standard System represents the Honeywell-recommended Experion PKS configuration that will provide customers with the best Experion PKS experience.

This configuration has been captured into a easy to use, single page reference document and can be found on HoneywellProcess.com.

To access the document please follow the Link:
https://www.honeywellprocess.com/library/support/Documents/Customer/Experion-Gold-Standard-System.pdf

VMware vSphere HTML5 Client & Adobe Flash End of Support

Honeywell currently utilizes the Adobe Flash-based vSphere Web Client for managing and administering virtualized systems on the VMware vSphere 6.5 release. The vSphere Web Client is also used on the legacy VMware vSphere 6.0, 5.5, and 5.1 releases which were supported for Honeywell systems. Adobe has announced an End of Support date for Flash on December 31, 2020, and all web browser developers will release updates to their software on or before this day which will prevent the use of Adobe Flash within the web browser.

To address this requirement, Honeywell intends to release support for the VMware vCenter 6.7 vCenter Server Appliance (VCSA) in Q3 2020. The use of the vCenter 6.7 VCSA will provide full management and administration functionality for supported Next Generation Premium Platform, Essentials Platform, and BladeCenter Premium Platform host servers. The following considerations apply to the use of the vCenter 6.7 VCSA:

- All Next Generation Premium Platform and Premium Platform HD systems must be upgraded to the latest EVIR410.3 Patch 1 baseline before the respective vCenter instance is upgraded to the vCenter 6.7 VCSA.
- The vCenter 6.7 VCSA is supported with VMware ESXi hosts running vSphere 6.0 or later. Hosts running legacy ESXi versions on vSphere 5.x or 4.x must be upgraded to vSphere 6.0 or later to enable vCenter 6.7 VCSA connectivity.
- Honeywell supports vSphere 6.0 and 6.5 for all legacy hosts which are also qualified and documented by Dell to be used on the specific server platform.

The use of the vCenter 6.7 VCSA will not include a migration of VMware ESXi host servers to vSphere 6.7. All Honeywell-supported host servers will remain at the currently supported vSphere releases and will continue to have access to vSphere Upgrade Manager for security updates. Note that the "Host Upgrades" functionality used for the Premium Platform is not available when using dissimilar vCenter and vSphere releases, hence the requirement to upgrade the Premium Platform environment to the EVIR410.3 Patch 1 baseline prior to deploying the vCenter 6.7 VCSA.

Honeywell intends to qualify and support the VMware vSphere 7.0 stack once the first cumulative update is available. Due to the anticipated timing of this release, the planned release and support for the vCenter 6.7 VCSA in Q3 2020 should provide ample time to perform the transition to the vSphere 6.7 appliance while minimizing the impact to other system components.

Honeywell recommends all customers start planning a migration to the VMware vCenter 6.7 VCSA to manage the pending End of Support for Adobe Flash. Please contact your Honeywell account team for additional details or for assistance in planning this activity.

VMware vSphere Model Number Updates

Starting in August 2020, Honeywell's model numbers for VMware vSphere solutions will be based on the VMware vSphere 7 product line. This change is necessary to align with VMware's vSphere 7 release, and the new model numbers will be documented in a revision to the HPS Virtualization Specification. The change in Honeywell's model numbers will not affect the vSphere releases supported with Honeywell systems at this time, and Honeywell's platforms will continue to be based on the vSphere 6.x hypervisor and vCenter versions noted in the specification document.

With this change, VMware vSphere licenses purchased from Honeywell will include:

- vSphere 7.x license key(s) associated with the software order
- vSphere 6.x downgrade key(s) for licensing Honeywell's virtualization platform hosts

Additional notes:

1) vSphere 7.x license keys included on the license certificate may be used once Honeywell has qualified and released support for vSphere 7 with Honeywell systems.

2) Honeywell intends to provide downgrade keys for vSphere 6.x for the duration vSphere 6.5 remains in the General Support phase.

Please contact your Honeywell account team with any questions relating to this model number transition.

TPS Release 42x Phase-out Announcement

TPS Release 42x was introduced in November 2009. The hardware platforms of GUS and APP dependent on TPS R42x were phased out in 2014, coinciding with end of support Windows XP and Server 2003 platform.

Effective June 15, 2020, TPS R42x, used in standalone TPN/TPS systems, is transitioned to phased-out lifecycle status.

Core TPS functions were rolled into Experion software and continue to be supported under Experion software releases.

Following this announcement, the TPS releases lifecycle status is as follows:

- R421.3 – Phased-out

Product Support Guide for standard HPS and HCI products is available in the Customer Resource Manual Tab PD23:

https://www.honeywellprocess.com/library/support/customer-resource-manual/PD23Z02A.pdf

Microsoft Windows 7 And Server 2008 R2 64/32 bit Operating Systems End Of Support – PMD Customers

After January 14, 2020, Microsoft has discontinued support for the Windows™ Server 2008 R2 and Windows™ 7 32/64 bit operating systems.

This means Microsoft will no longer generally distribute security patches for Windows 7 or Server 2008 and stop providing non-security hot fixes, online technical content updates or telephone support.

How does this affect our PMD customers?

As patches are developed for Windows 10 and Windows Server 2016, this will expose to vulnerabilities that existed on Windows 7 and Windows 2008 Server. Systems that continue to operate on unsupported software are at risk to cyber-attacks.

Additionally, the Honeywell support policy dictates that the support of R83X will be discontinued by end of 2020. After this, Honeywell will only provide commercially reasonable support for these systems. For customers on R900.x, their Design Module (DM) is still running on Windows Server 2008 32 bit (Virtual)

and Windows 7 Pro 32 bit (Physical). This DM will also be subject to cyber and security risks due to unavailability of OS updates and limited support from Honeywell.

How do we help our customers?

Microsoft will provide extended service support (ESU) for up to 3 years through Honeywell to support PMD Server and HMI nodes running on R83x.

This announced extended support with security patching is valid for up to 3 years. The trigger date is January 2020. Security Patches are cumulative, therefore the fee is an annual payment for the full year regardless of which month the program is joined.

Honeywell will continue to test the Microsoft OS patches for extended support services customers. This is a temporary solution to address the Windows obsolescence risk. Preferred solution is to migrate the system to latest Experion PMD R91x series. This program only applies to embedded OS, which means the OS was purchased from Honeywell along with a Honeywell product.

Below are the prices that will be charged to customers for buying ESU for each PMD HMI and Server nodes running on R83x.

	2020		2021		2022	
Windows 7 For Embedded Systems(64 bit)	Contract (SESP/BGP) $200	No Contract $260	Contract (SESP/BGP) $400	No Contract $520	Contract (SESP/BGP) $800	No Contract $1040
Windows Server 2008 R2	Contract (SESP/BGP) $2700	No Contract $3500	Contract (SESP/BGP) $5400	No Contract $7000	Contract (SESP/BGP) $10800	No Contract $14000

For Design Module which uses Win7 and Win 2008 Server 32 bit OS, Honeywell will qualify DM with Win10 32 bit OS to support customers running on R83x and R90x.

Honeywell will work with customers to upgrade their DM to Win10 32 bit OS and ensure all relevant architectural risk are mitigated as part of that. Customer will have this option available in 2021 and hence DM migration should be planned based on that.

While this is a stop gap measure for the next three years, the long-term solution is modernization to the Experion PMD R91x release. In addition, Honeywell will further explore the opportunity to Upgrade DM to 64 bit which will allow to run DM on Windows Server 2016 OS and provide better virtualisation and life cycle support.

Below is the short summary of overall Honeywell recommendations to reduce the risk of unplanned downtime for R83x/R90x customers running PMD nodes in Windows 2008 Server and Win 7 OS :

a. Experion PMD Server, HMI and DM upgrade to Experion PMD R91x or later which is based on Microsoft Windows Server 2016 & Windows 10 Operating Systems for a longer lifecycle support.

b. Customers to buy ESU for PMD Server and HMI as provided by Microsoft, valid for 3 years and priced as mentioned above. **However, before buying ESU, customers have to ensure that they have planned migration to latest PMD release in next 3 years or booked a lifecycle migration contract.** For e.g. if the migration is planned in 2022, then ESU needs to be bought for both 2020 and 2021.This is a temporary stop gap arrangement to address Windows obsolescence risk only.

c. For Design Module, customers should upgrade to Windows 10 32 bit OS until they plan to move to latest PMD R91x release.

d. Run a Cyber Security Vulnerability Assessment to help identify and prioritize OS and other security vulnerabilities that may exist and then implement appropriate solutions to help protect from threats

Honeywell looks forward to working with you to help ensuring that your system remains reliable and secure well beyond the Microsoft End of Support deadline.

For more information on ESU pricing, eligibility criteria for customers and all relevant information, please contact Michael.Khilla@honeywell.com, Harri.T.Oksanen@honeywell.com **and** amit.singh3@honeywell.com

Experion R4xx: Certain Scenarios Installing MS Security Update Dec 2019 or Jan 2020 ISO May Cause Windows to Fail

Background:

During the December Security Roll-Up qualification, Honeywell testing found that installing an MS update using December 2019 or January 2020 ISO on Experion R4xx caused operating system to crash on a system where July 2019 ISO or earlier was installed. The issue has been reported to Microsoft.

Applicable Experion Release:

Experion R4xx installed with MS ISO July or earlier

Workaround:

First install MS update using Nov 2019 and then install MS update from Dec 2019 or January 2020 ISO.

Solution:

The problem has been resolved in MS ISO March 2020 and later, only available to ESU customers. Non-ESU customers must still use the November ISO before deploying January 2020 ISO.

Using a Read-only Domain Controller on Level 2 Might Impact Experion Robustness & Domain Architecture Considerations

Introduction:

Reliable Windows authentication is key to a robust Experion system. Outside of operator's logging in, there are lots of other authentication activities happening in the background and losing the ability to authenticate is a significant loss and should be protected against.

For control systems, having a functional authentication is a critical function that needs to be considered with the right system architecture.

Read-only Domain Controller (RODC) and Windows Authentication

As per Microsoft design RODCs are dependent on Read-Write DC (RWDC) for an authentication, in a scenario where an RODC would be configured on L2 and a RWDC on L3, any authentication required by Experion would be passed from L2 to L3, which would make Experion vulnerable if in case of a network disruption to L3 or if the L3 Domain Controller is unavailable (e.g., applying security update, reboots, etc.).

In more detail, for authentication a writable DC is required, hence all Experion authentication is going to the L3 DC. Some Active Directory (AD) queries server as part of operator login and operator or group configuration in Experion will be able to be handled by the RODC, but the actual authentication for operator security and for any other reason will go to the L3 DC.

RODCs will refer authentication request onto a Read-Write (RW) DC and may cache these credentials for future authentication depending on policy, so to be sure authentication succeeds an RWDC needs to be available <u>all the time</u>.

An RODC can handle many other AD read requests where the call permits it, but many of the Windows AD API calls require a flag be set advising that using an RODC is permitted where available, and some calls do not provide this option and thus always require an RWDC even for a read operation.

One advantage of an RODC is that it reduces the replication traffic since it is not two-way but one-way from an RWDC to the RODC; however, this advantage is outpaced by the impact on authentication robustness.

Impact on Experion

A failing or slow Windows authentication would impact the entire Windows infrastructure and applications using it. As a consequence, multiple applications and Windows functions would be impacted.

From an Experion angle, RPC call failures and timeouts would be expected, impacting Experion core functions like OPC, DSA, Console Station Synchronization processes, etc.

Similarly, loss of Level 3 domain connectivity could impact multiple Experion clusters for topologies where multiple Experion clusters with RODC share a common Level 3 DC.

This is the reason why we are recommending a robust Windows domain infrastructure, the Experion documentation would be enhanced to cover this topic in similar details.

Recommendations

Here are high level architecture guidelines:

- We are recommending systems to be configured with at least a peer domain controller, with a fully functional Domain Controller (RWDC) on Level 2.
- At least 1 RWDC per L2 FTE Community
- When using sites, each site should have at least one read/write DC.
- L3 Domain Controller must have the System Management Services disabled (when installed)

Changing from RODC to RWDC

Here are the high-level tasks to switch from an existing RODC to RWDC:

- Demote RODC
- Run the Meta data clean-up procedure from writeable DC
  (follow https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/deploy/ad-ds-metadata-cleanup)
- Promote as a writable DC

Understanding the "Experion Local Control Network (ELCN) Unified Engineering Tools" New in R511.3

HPS Technical Support wanted to highlight a new function introduced in Experion R511.3 for TPS integrated customers.

Later in this document we are also providing steps to enable the CDA interface on EHPMs for customers who licensed the CDA integration. This process would need to be done after a migration to R511.3 or later in order to utilize the new Engineering Tools. Refer to the documentation for detailed instructions to import the TPS points using the new ELCN Database Import Utility even though the CDA interface has already been configured in Control Builder on an Experion release < R511.3.

From the Experion R511.3 SCN:

Beginning with Experion R511.3, the Experion Engineering Tools facilitate ENIM point configuration. Experion Engineering Tools can be used to perform most of the Native Window Data Entity Builder operations for ENIM nodes. Unified Engineering Tools provide an environment having consistent user experience in the unified Experion system. Some of the engineering operations that can be performed are:

- Creating node platform blocks
- EHPM node-specific configuration
- Configuring IO modules
- Channel and point building
- User programming (PM/CL)
- Modification and deletion of the channels and points

ELCN Database Import Utility is added to the Experion Engineering Tools set for transferring Local Control Network (LCN)/Enhanced Universal Control Network. (EUCN) point configuration data to Experion databases.

The unified Experion system leverages a common platform framework which is supported on a common system specification resulting in reduced deployment time and complexity. The following are the benefits of the unified Experion system:

- Provides a consistent user experience for all configuration tasks.
- Ease of migration of database from EUCN to the unified Experion system.
- Increase in productivity in accomplishing configuration tasks, as well as user programming.
- Reduces qualification efforts on different flavors of engineering user station specifications.
- Reduces training needs on Native Window and Data Entity Builder operations.

For more information on Unified Engineering tools, refer to *ELCN Unified Engineering Operations Guide.*

Important things to remember:

The Windows user that would be performing the checkpoint import/engineering must be a member of the Engineer group (domain or locally).

Auto Import also has some new requirements: Needs TPS File Transfer installed and configured on the ESVTs.

An easy way to use the new ELCN Database Import Utility would be to create a folder off of C:\temp called EHPM_DB (e.g., c:\temp\EHPM_DB). In this location, we put (using TPS File Transfer) all of the checkpoint files from the NET>&Ixx directory (for example an EHPM on UCN4) and we would copy all of the files from NET>&IO4 to the c:\temp\EHPM_DB directory. In addition to these files, you also must copy (required for the import tool to work properly) the current NET>&ASY>NCF.CF file to the C:\temp\EHPM_DB location. Then, run the ELCN Database Import Utility. We would use this method in the example below. Once collected the dataset can be validated with the ELCN-Import-Utility-Validator-for-R511.3 (link at the end of the document).

When using Control Builder to engineer TPS points, it is important to remember to use an EST, with Native Window running (as ENGR) and with the Engineering Menu active on Native Window.

The EHPM's CEE is not a functional CEE, but only a Control Builder container, it cannot be activated, therefore its color would remain blue on the monitoring tab as shown below.

Use Case: Configure an EHPM for Experion Integration (CDA Interface)

1) On Experion R511.3 (or later), login as a Windows User member of the Engineer group (locally or domain)

2) Verify that the TPS File Transfer is configured and running on ESVT A and B.

3) Verify using Ctools that the EHPM is running with the most current firmware (Experion Boot and App Firmware flashed) for Experion R511.3. If not, you first need to upgrade the Experion Boot and APP F/W to the Experion R511.3 version.

4) In our example the EHPM #29 will be configured for Experion Integration (CDA interface)
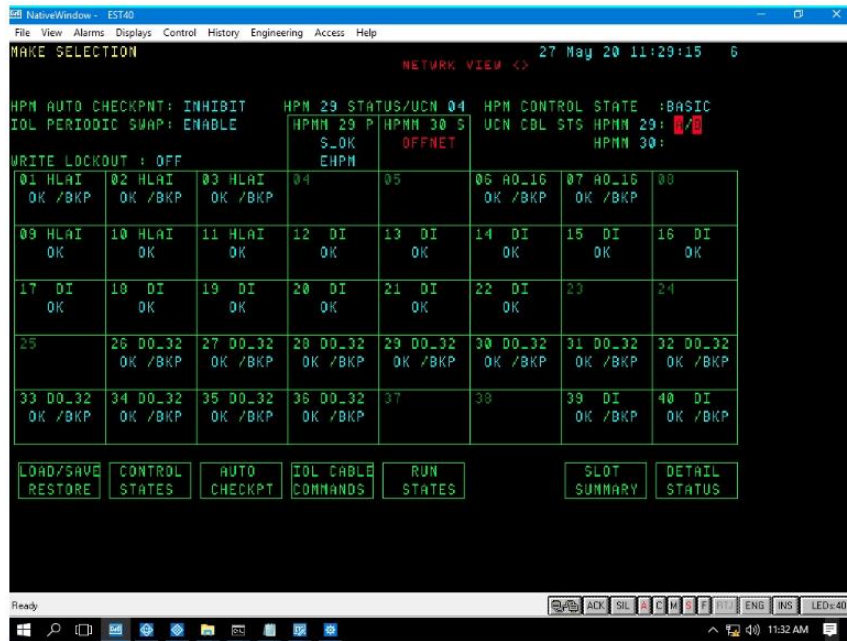

 5) In Control Builder configure EHPM block with same configuration UCN node number, FTE address, etc. In our example the EHPM block created was named L1U4EHPM19, and a CEE container object is automatically created.

6) On the EHPM block configuration, disable temporally the automatic point import.

7) In Control Builder, load new EHPM from project to monitoring.

8) Create folder c:\temp\EHPM_DB\ on the Experion server or an engineering station, using TPS File Transfer to copy all the files from NET>&IO4 to c:\temp\EHPM_DB directory. In addition to these, you also must copy (required for the import tool to work properly) the current NET>&ASY>NCF.CF file to the C:\temp\EHPM_DB location.

9) Run the ELCN Database Import Utility (do not use the point import utility, refer to the user manual for details). Configure the Base Name of Server Experion Cluster (no A/B) and select connect.
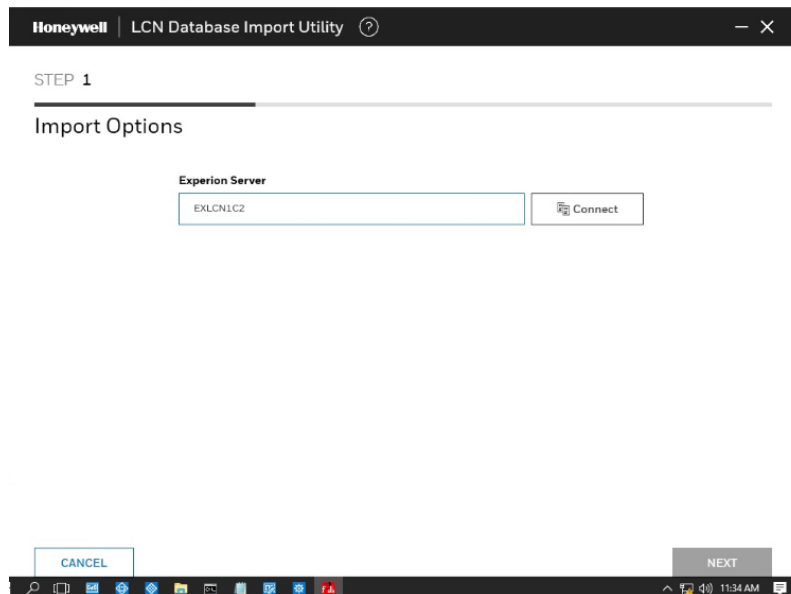
10) Select Checkpoint and then NIM.
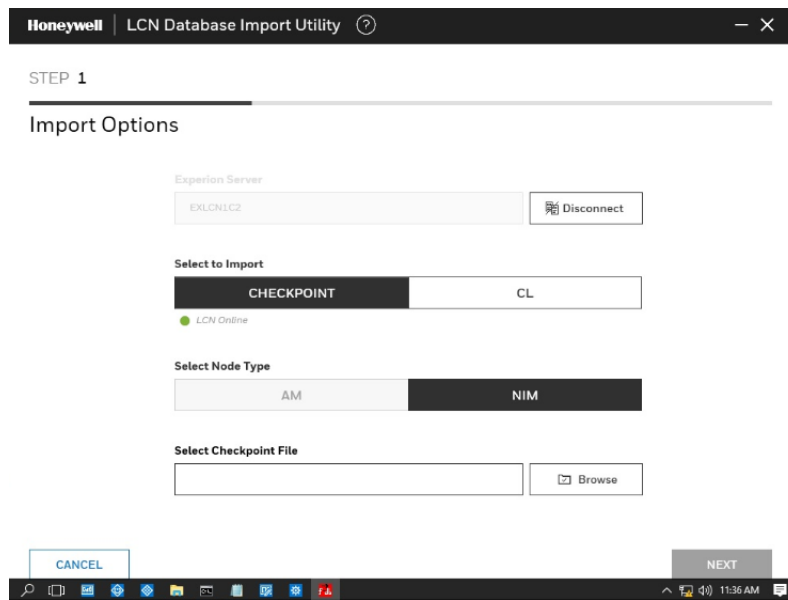
11) Select browse and navigate to c:\temp\EHPM_DB\ and select the appropriate checkpoint file

Verify that the NCF.CF is present in the same folder, the file is required for the tool to work correctly.

12) Select the EHPM created as in Control Builder, L1U04EHPM19 in our example, select next.
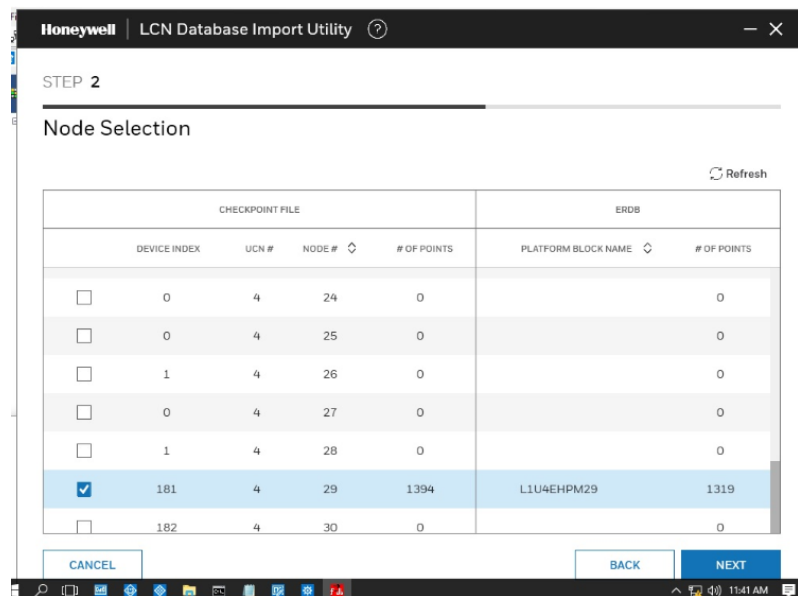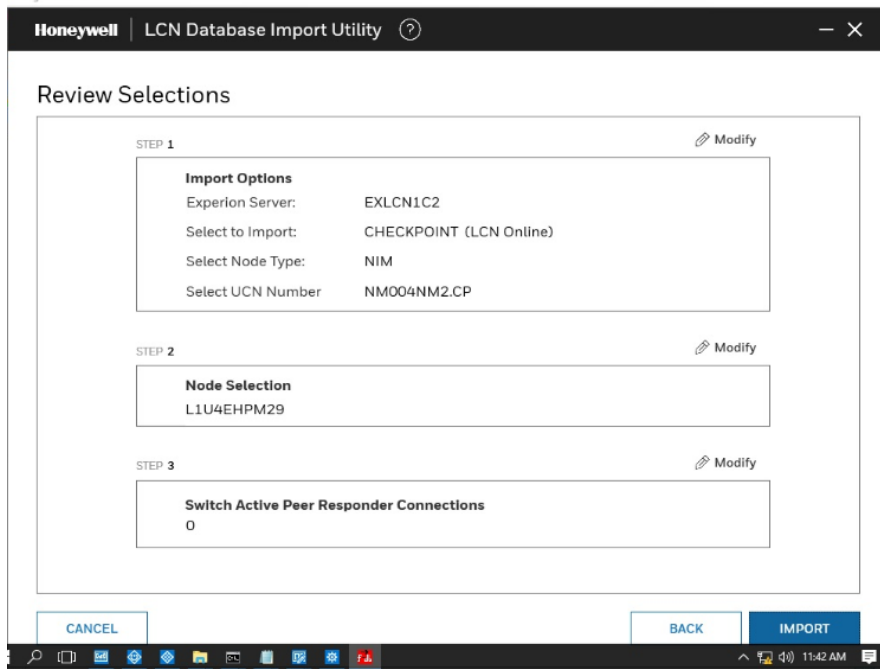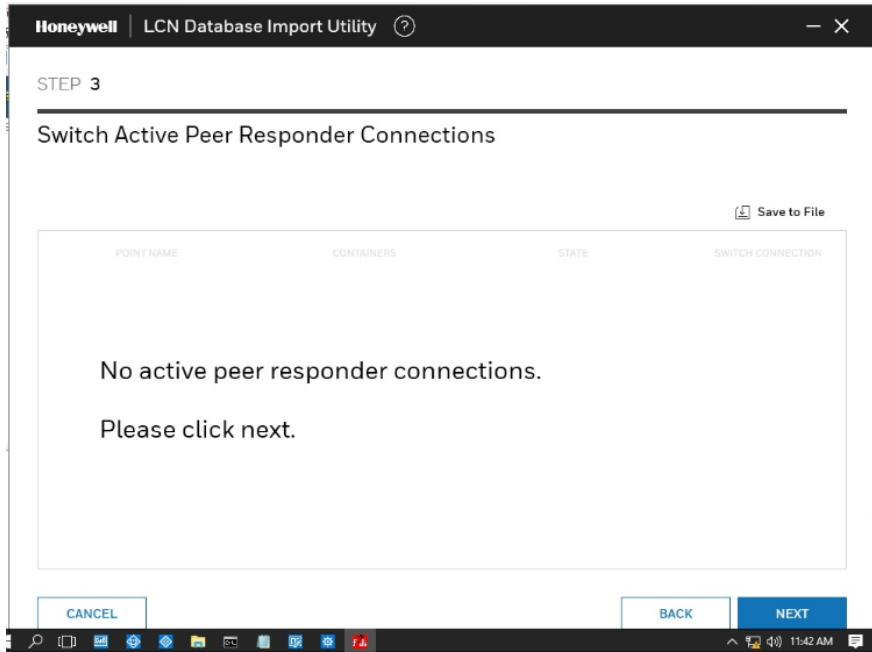
13) Confirm import by clicking on YES
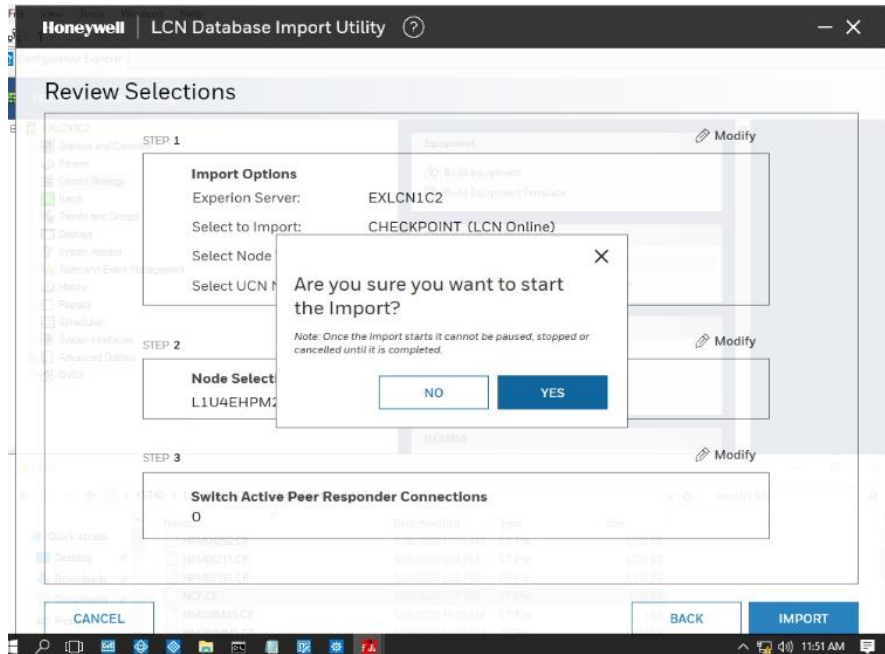
14) Wait for process complete
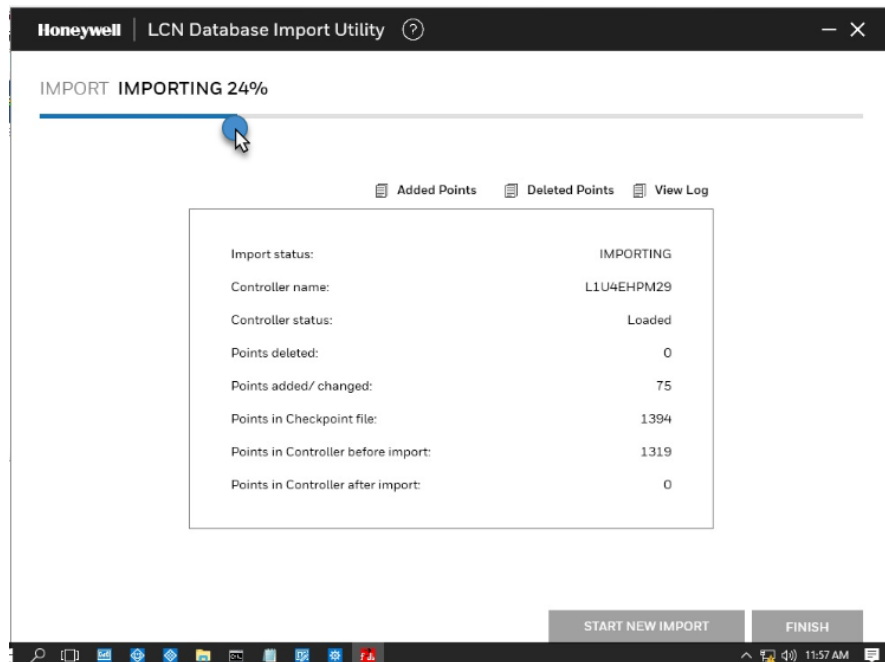
15) Control Builder Project/Monitoring will be populated automatically, adding IO and points
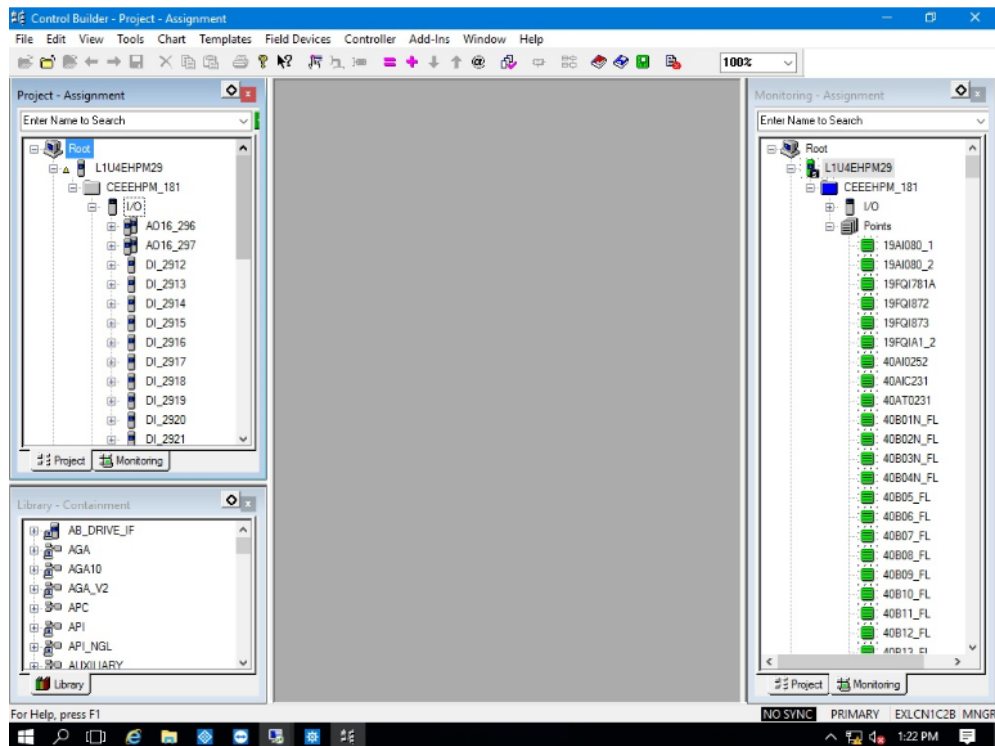
16) Tags will now have the same configuration as what you would find in Native Window
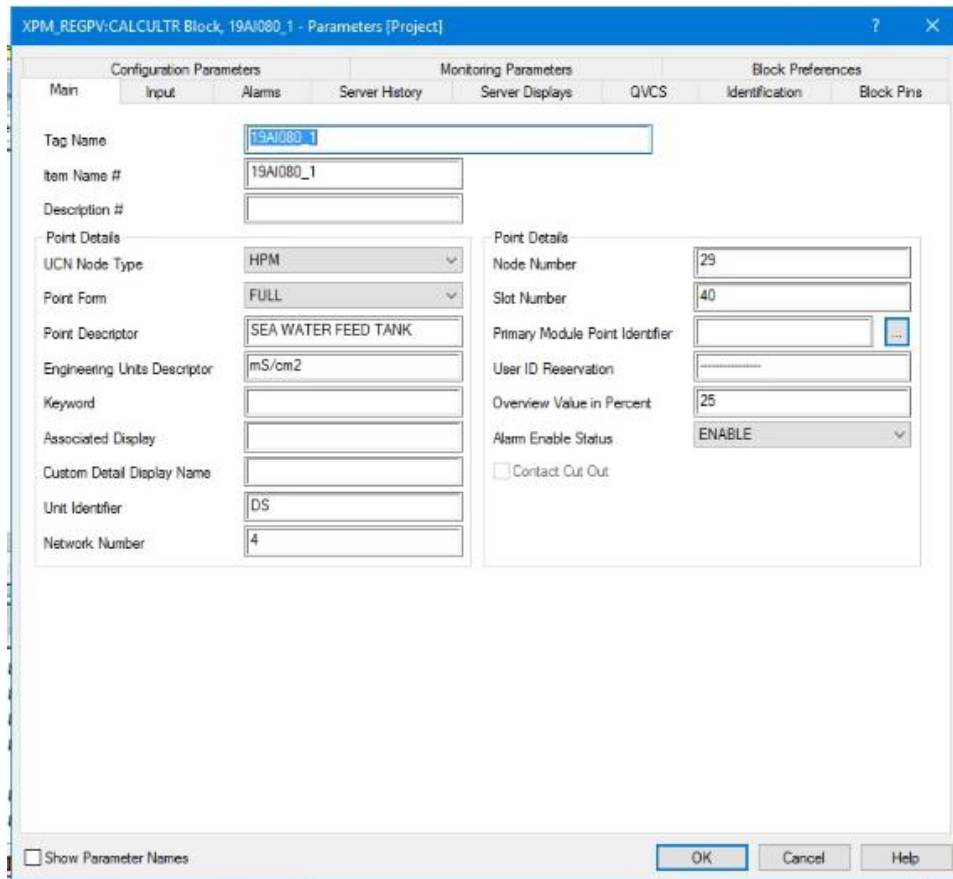
17) Finally, enable Automatic Point Import

If required, the ELCN Import Checker Tool utility (link below) can be used to validate the checkpoint/NCF data set before importing into production system.

Related Content

https://www.honeywellprocess.com/library/support/software-downloads/Experion/ELCN-Import-Utility-Validator-for-R511.3.zip

https://www.honeywellprocess.com/library/support/Documents/Experion/Experion-LCN-ELCN-Engineering-Operations-EPDOC-X639-en-511A.pdf

How to Change Default Control Confirmation Selection in Station From Yes to No

Content

Question / Problem	Site has configured setpoint tolerance for CDA points and they want to know, if possible to change default setpoint tolerance popup message value selection from 'Yes' to 'No' button?
symptoms	Documentation issue
Answer / Solution	Experion install system, default select 'Yes' on popup message for change confirmation, to change it to 'No' need to perform below setting Navigate to Server wide settings page -> under Control confirmation -> select 'Default control confirmation response is NO' This will set change confirmation popup message default selection to 'No' button.
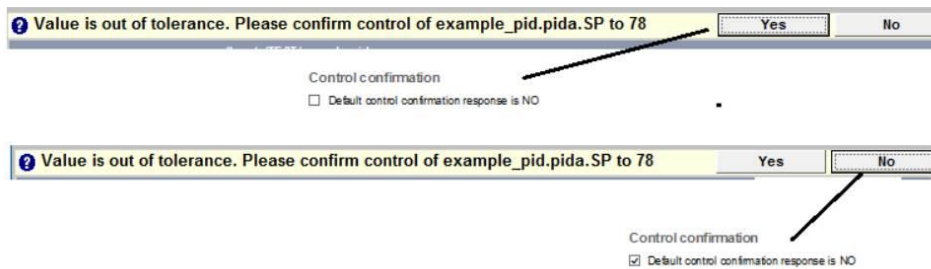
Change to the Way We Access the System Inventory Portal

On June 5, 2020, a change was implemented to the login process for the HPS website that affects how users access services such as Support, System Inventory, Assurance 360, Migration Assistant, Spare Parts Online (Buy Now) eCommerce and the Channel Partner Portal. Honeywell IT made these changes in order to maintain the highest level of security in our online services.

What Has Changed?

The change requires the user to login a second time when accessing these services. Should you need assistance, please contact the Honeywell Web Support Team HPSWeb@Honeywell.com

Logging into the portal now requires the following process:

1) Go to www.honeywellprocess.com/ and login.
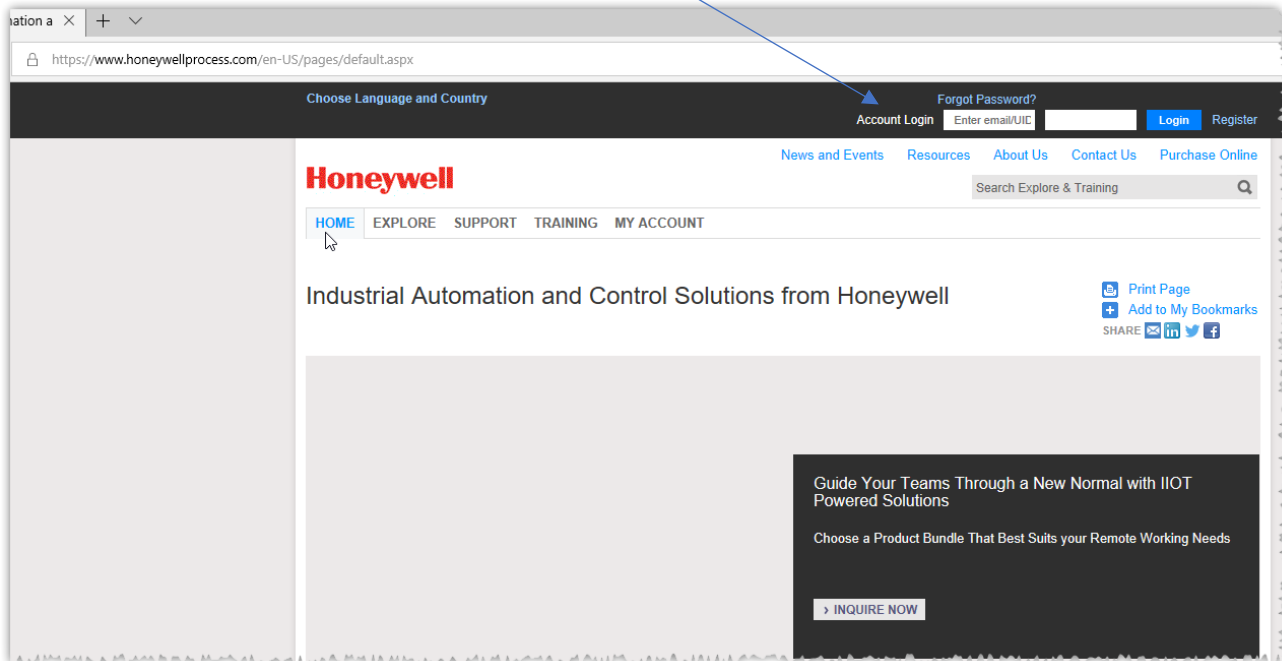
2) After login, user sees this message.
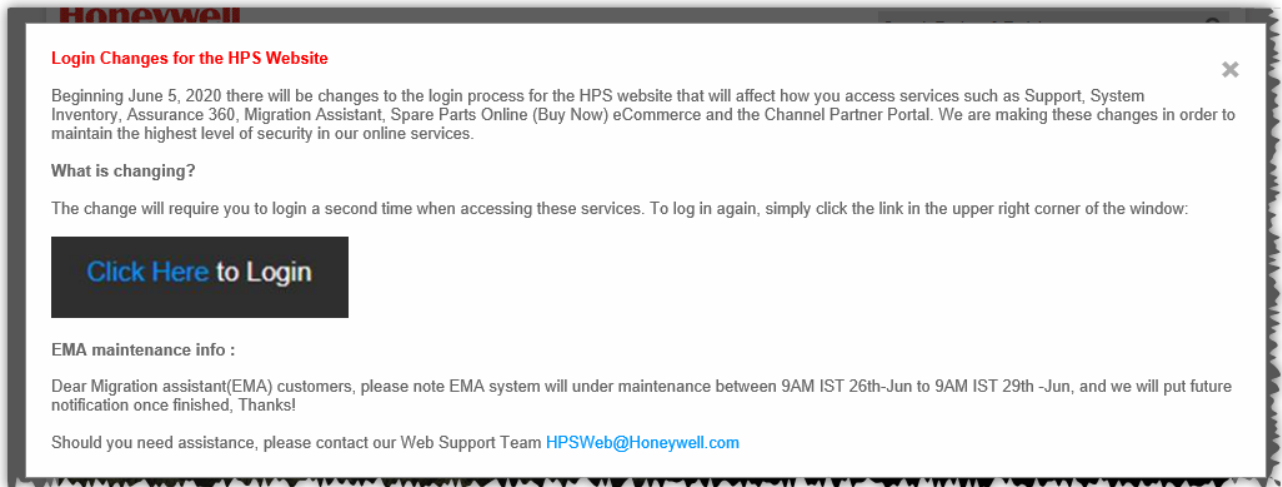
3) Select **Support**
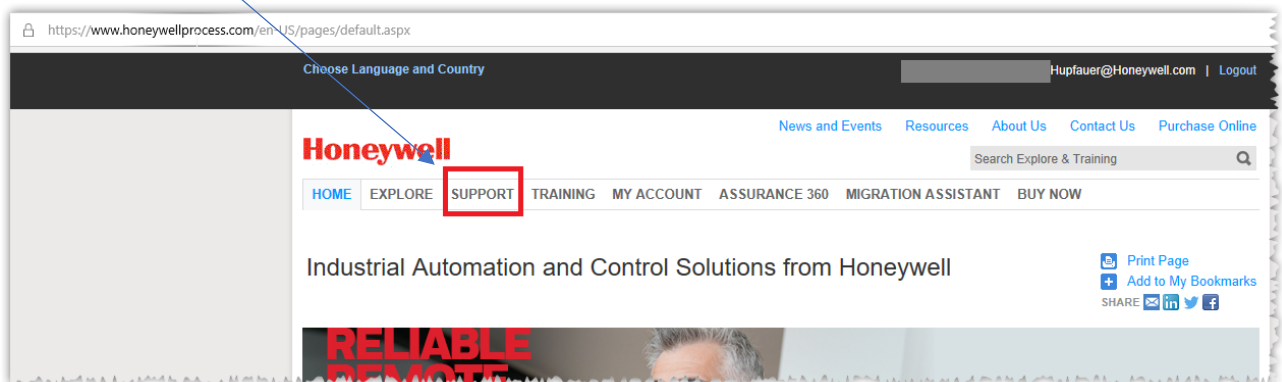
4) Notice the submenu appears; however, the user is no longer logged in. The user must login again…this is AS DESIGNED.
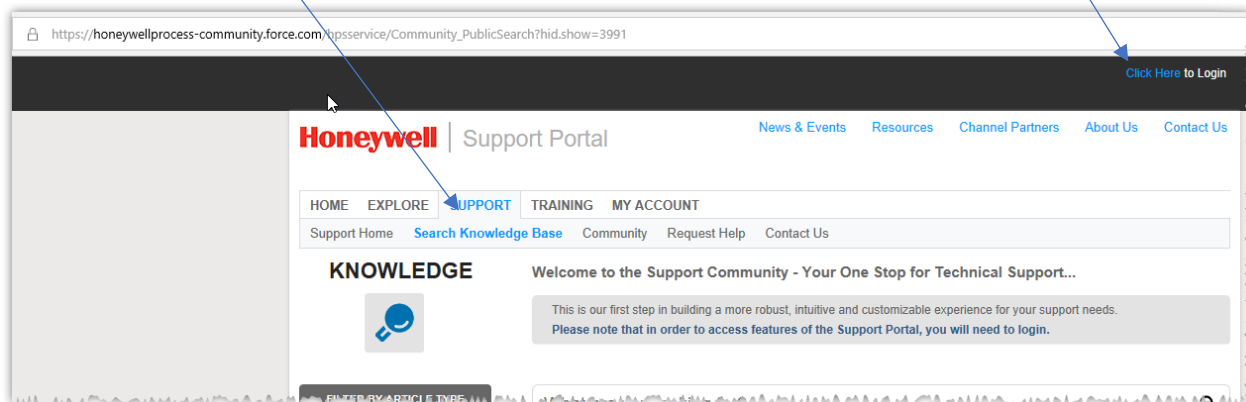
5) After logging in for the second time, **System Inventory** appears
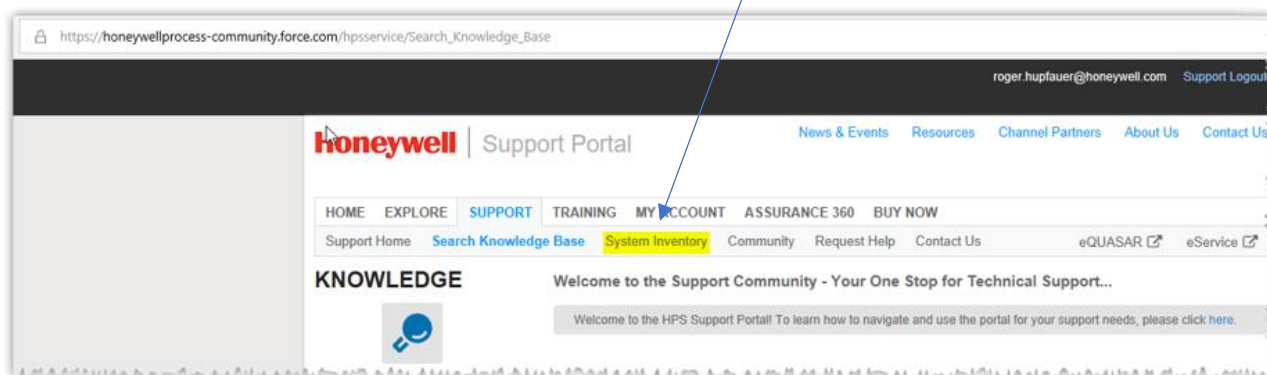
System Inventory Tool R300.1 Available

The System Inventory Tool (SIT) R300.1 is now available for download from the System Inventory Tool Landing Page. This self-service tool can be installed on Experion PKS R400.8 or newer systems to scan the inventory details of the entire system, including network, Cisco switches and associated nodes at predefined intervals. The tool generates an inventory file that users upload to the Support Portal to see their inventory details in a logical and graphical overview, which is used to support Honeywell's automated online contract renewal process.

Provided at no cost for all Honeywell customers, both contracted and non-contracted, the SIT runs in the background and will not impact control system performance.

Once the SIT has completed its scan, a .cab file is created and then either the Honeywell technician or the customer uploads the inventory file to the System Inventory Portal. The portal will display the licensed software sourced from Honeywell, shipped hardware sourced from Honeywell, and inventoried asset data collected by the System Inventory Tool.

New in R300.1

- Advanced solution support on Level 3 (L3)
- Additional support for QCS
- Support for Experion PMD
- Collect inventory for all network switches supported by Experion

- Improvements to the diagnostic tools to quickly detect and report on SIT failures (includes SAT and device discovery)
- Reworked device discovery
- Progress meter during the collection phase
- Profit Suite (APC) support
- Control Performance Monitor CX support
- Control Performance Monitor standard support
- Profit Blending Suite support
- Profit Movement Suite support
- DynAMo Alarm Management Suite support
- Uniformance Asset Sentinel support
- Matrikon OPC Servers support (see **Appendix A** for full list)
- UniSim Competency Suite support on L3

Appendix A

Matrikon Data Manager
Matrikon Desktop Historian
Matrikon OPC Server for GE Turbines
Matrikon OPC Funnel
Matrikon OPC Security Gateway
Matrikon OPC Server for Allen Bradley
Matrikon OPC Server for APACS Direct
Matrikon OPC Server for BACNet
Matrikon OPC Server for Bailey DCS [Infi 90]
Matrikon OPC Server for Citect
Matrikon OPC Server for Foxboro DCS
Matrikon OPC Server for GDA [ODBC]
Matrikon OPC Server for GE PLCs
Matrikon OPC Server for IEC 61850/61400-25
Matrikon OPC Server for IP21
Matrikon OPC Server for Johnson Controls N2
Matrikon OPC Server for KNX
Matrikon OPC Server for LonWorks LNS
Matrikon OPC Server for MarkV Direct
Matrikon OPC Server for MarkVI Direct
Matrikon OPC Server for Mitsubishi PLCs
Matrikon OPC Server for Modbus
Matrikon OPC Server for Moore APACS (API)
Matrikon OPC Server for Omni Flow Computers
Matrikon OPC Server for Omron
Matrikon OPC Server for OpenBSI
Matrikon OPC Server for ProRAE
Matrikon OPC Server for Provox (Direct)
Matrikon OPC Server for ROC
Matrikon OPC Server for RS3 RNI
Matrikon OPC Server for SCADA DNP3
Matrikon OPC Server for SCADA IEC 60870
Matrikon OPC Server for SCADA Modbus
Matrikon OPC Server for SCADA MOSCAD

Matrikon OPC Server for Siemens PLCs
Matrikon OPC Server for SNMP
Matrikon OPC Server for Vestas
Matrikon OPC Server for Wonderware InSQL (Wonderware Historian)
Matrikon OPC Server for Wonderware Intouch
Matrikon ORB
Matrikon OPC UA Tunneller – UA Proxy Component / UA Proxy
Matrikon OPC UA Tunneller – UA Wrapper Component / UA Wrapper

Installation

The SIT R300.1 is a standalone installation, and therefore not integrated with the Experion R511 media package.

While the SIT can be installed on Level 2 (L2) and Level 3 (L3), the installation and configuration on both levels are independent of each other. As such, users can choose to install the tool on either or both levels, based on their control system requirements.

Functionality of SIT on L2 and L3
Key features & differences on both levels

L2

COMPONENTS INSTALLATION
Two components are installed.

1. SIT User Interface
Installed only once on the entire network on either ExperionPKS Flex or Console Station.

2. SIT Data Collector
Installed on each Redundant Server (B) or Non-Redundant Server.

DATA COLLECTION AND MONITORING
1. Data Collection
Each SIT Data Collector installed gathers data from the servers and provides it to the SIT User Interface.

2. Data Monitoring
The data collected is then monitored in the SIT User Interface.

L3

COMPONENTS INSTALLATION
One component is installed.

1. SIT User Interface
Installed only once on a single Non-Experion node on the entire network.

DATA COLLECTION AND MONITORING
1. Data Collection
Data is collected remotely by deploying agents in the nodes of domains.

2. Data Monitoring
The data collected by the agents is then monitored in the SIT User Interface.

Information for R230 Users

Users who have installed the R230.1, R230.2 or R230.3 versions of the SIT should upgrade to R300.1 to ensure they have the latest support from Honeywell (unless they are currently running Experion R3xx.x, which is not supported by SIT R300.1). During the upgrade, their current SIT configuration will be retained.

Experion Compatibility

SIT Version	Supported Experion Version
R200.1	R301, R310, R400 and R430
R200.2	R301, R310, R400 and R430
R200.3	R301, R310, R400 and R430
R210.1	R3xx.x to R510
R210.2	R3xx.x to R510
R220.1	R3xx.x to R510
R230.1	R3xx.x to R510
R230.2	R3xx.x to R510
R230.3 (SIT patch must be installed on 32bit systems after R230.3 installation)	R400.8 to R511
R300.1	R400.8 to R511

QCS Compatibility

QCS Architecture Version	Experion PKS Layer	System Inventory Tool Release Support
RAE1xx	None	
RAE2xx	None	
RAE3xx	None	
RAE4xx	R101/201/210	No support
RAE5xx	R300/301/310/311	No support
R6xx	R 400.8	R300.1
R7xx	R5xx	R300.1

What is SIT and Why Do You Need It?

Overview

The System Inventory Tool (SIT) provides a comprehensive system inventory documentation solution to support Honeywell's contract renewal process. The tool enables our customers to complete their yearly contract renewal online through an automated system, better manage risk, prepare for any migrations, and ensure compliance and continuous evolution of their control system.

The SIT collects asset data, which is then hosted in a secure Honeywell data center where the customer can view all their control system asset information (both hardware and software) through the System Inventory Portal. And, best of all, the tool is provided free of charge by Honeywell for all contracted and non-contracted sites and does not require an SESP contract or Assurance 360 service agreement.

Automated Online Contract Renewals and More

The SIT was developed to support online contract renewals. Gone are the days of the laborious task of manually reviewing contract renewal worksheets, trying to track changes via emails and phone calls, and providing results in a timely manner. No more lost notes or questions such as, "What did we do last year?" All updates and notes regarding asset quantities will be captured in the tool and carried forward year over year, making future contract renewals faster and easier. But contract renewals are just once a year—what else can you do with the tool?

Better Management of Risks

With the SIT, you have the ability to see all your control system assets by each MSID in the Honeywell System Inventory Portal. With this view, product support status is shown for each asset. Do you know if your control system is using outdated equipment or assets no longer supported by Honeywell? Finding answers like this is just a mouse click away in the portal.

When you can see all your equipment in a single view via the online portal, you know exactly what hardware and software are running, what is outdated and where improvements could be made—thus better managing risk.

Compliance and Continuous Evolution of Control Systems

With the asset topology feature found in the System Inventory Portal, you'll have insight into the hardware components in each control system, thus avoiding lengthy delays to gather the right information when the system needs to be supported or expanded.

Today, control systems are more complex than ever before and there is limited information on how the different components need to interact. When you can visualize your entire system in one view, you increase awareness that leads to better decision-making.

Migrations

You have a budget for a migration, and in many cases it's "use it or lose it." So, how will you know where best to invest in your control system? Can you quickly review every MSID design, topology and product support status for every asset? If you've uploaded your inventory asset data file to the System Inventory Portal, all this and more are just a mouse click away. And did we mention it's free? That's right—Honeywell offers this to all our customers at no cost. No contract or service plan of any kind is required.

Honeywell Updates

System Name : M████4   MSID : M████4   Product Name : Experion Server

Update Name

++ Patch Experion PKS R410.2 Honeywell Security Model - Workstation

++ Patch Experion PKS R410.2 Honeywell_HCI_Runtime

++ Patch Experion PKS R410 QBP Patch1

++ Patch Experion PKS R410 HMIWeb Station and Display Builder Patch 2

++ Patch Experion PKS R410.2 Configuration Studio Patch 1

++ Patch Experion PKS R410 Server Patch 7

++ Patch Experion PKS R410.2 Controller Patch

++ Patch Experion PKS R410.2 Honeywell_Safeview

++ Patch Experion PKS R410.2 Honeywell System Management Runtime

Quickly Locate Assets

All assets are listed by Site > MSID and user-defined system names, and because each system name you choose is assigned to its respective MSID, finding your systems is easy—even if you don't know the MSID name.

What Can the Collected Asset Data Tell You?

Keeping track of the patches and updates you've installed on your servers and stations can be a time-consuming task. It requires logging into each server or node and checking through the control panel to see which patches and updates have been installed.

Now, if you've run the SIT and uploaded your asset inventory file to the portal, just click on the server or console station and a complete list of all installed applications, patches and updates will be displayed in an easy-to-read table.

Need to find out which version of boot firmware is installed on a C300 controller? Just click on the MSID, select the controller and a table will display everything you need to know. Want even more flexibility? Export the data to an Excel spreadsheet and sort it or create a pivot table for convenient viewing.

What Data Does the Tool Collect?

The SIT is designed to capture details of the existing system hardware and software versions, including servers, stations, controllers, I/O modules, node details, installed applications, and switch models.

How Can You View Your Data?

The System Inventory Portal allows customers and certain Honeywell account managers to see their account asset data. Within the portal, you can see all your servers, stations, controllers, nodes, and switch hardware, as well as detailed information about each. Depending on which asset you're viewing, you can see the serial number, F/W, BIOS, installed software, support status, and much more.

To access the portal, go to honeywellprocess.com/support and login with the same credentials used when you registered.

Not registered? No problem! Registration is free and takes less than a minute. Once you are registered, login and select the Support tab, then select the System Inventory tab.

Who Can See Your Data?

All inventory data is viewable by only the customer, the customer's account manager, and Honeywell GTAC. In the event you call for support, GTAC can quickly get needed information such as F/W version, BIOS version, hardware rev, etc. Nobody else can ever see the data—not even other Honeywell employees.

What Data are Collected?

When you log into the System Inventory Portal, you will see a list of your sites. Select a site and there are three icons: Licensed Software, Shipped Hardware and Inventoried Assets.

Licensed Software	Shipped Hardware	Inventoried Assets
List of all licensed software shipped by Honeywell to the customer. Includes TPS BLDR, EBR, Experion PKS, GUS, PHD, and DOC 3000 licenses.	A complete list of every piece of hardware shipped by Honeywell to the customer, sorted by most recently shipped. Includes product part number, description, serial number, and date shipped.	Comprehensive list of all assets on each control system. Includes servers, stations, controllers, LCN nodes, and switches.

Used by Customers Worldwide

Today, Honeywell has over 900 sites worldwide using the SIT in more than 2,500 control systems. Many customers have reported that the tool is easily installed, runs flawlessly, and the time saved via the automated contract renewal process eliminated weeks of manual audit work. What used to be a tiresome and lengthy process can now be completed automatically, with 100 percent accuracy and in less than a day.

Helpful Links

The System Inventory Tool and portal are available at https://www.honeywellprocess.com/support.

https://www.honeywellprocess.com/library/marketing/notes/System-Inventory-Tool-What-is-it-and-why-I-should-be-using-it.pdf

System Inventory Tool: Is it Safe to Use in My Control System?

The System Inventory Tool (SIT) is a self-service tool that HPS customers install on an Experion Flex or Console Station, along with data collectors on the Experion B Server (or non-redundant node) to collect asset data at Level 1 and Level 2, which is used to support Honeywell's automated online contract renewal process.

The SIT generates an inventory file (.cab) that either the customer or Honeywell Field Support Specialist uploads to the secure System Inventory Portal where the user can see inventory details in a logical and graphical overview.

This tool is safe for use on your control system. It runs as a low-priority Windows Service Event, which means it will throttle down or even pause if other Windows Events need to take priority. As such, the tool will not put a burden on the control system, nor adversely affect the performance of the network or control system.

The SIT does not collect any sensitive data. No IP addresses or customer information are ever collected. The data collected are strictly related to the assets (e.g., BIOS version, F/W version, model number, serial number, H/W version, and other asset-only related information).

System Inventory Tool Security

🔒 **Does not collect sensitive data**
No IP addresses, MAC addresses, or any sensitive network information

🔒 **Cybersecurity**
Secure authentication on HoneywellProcess.com
Enhanced security and support via TLS 1.1 or higher

🔒 **Honeywell Data Governance team**
Data access highly restricted and protected via Encrypted two-factor authentication

From January 2018 to May 2020, there was a 79 percent increase in SIT adoption worldwide for contracted sites, with over 1,000 sites now using the tool without incident. The time saved via the automated contract renewal process eliminated weeks of manual audit work; what used to be a lengthy, rigorous process can now be completed automatically, with 100 percent accuracy and in less than a day.

Summary	Contracted Sites			
Pole	# of sites	# of sites using the tool	% of sites using the tool	change since Jan 2018
AMER	663	559	84.31%	45.95%
APAC	128	91	71.09%	167.65%
EMEA	486	384	79.01%	78.60%
Global	1277	1034	80.97%	78.89%

When it comes to the performance impact on a running control system, the following table summarizes typical system configuration CPU usage and time to complete. As you can see, CPU impact is typically in the single-digit percentage, and the time to process data is minimal. Keep in mind that time to process will vary based on the size of the control system; number of nodes; and number of controllers, switches, servers, and stations.

Node type	System configuration	Average additional % CPU used	Time to complete audit	Number of PCs being audited
ESVT – Server B	• Dell PowerEdge R710 server • (8) Processors: Intel(R) Xeon(R) CPU E5620 @ 2.40GHz • Speed: 2,394 • 12 GB RAM	Negligible	7 minutes 52 seconds to 11 minutes 33 seconds	4 PCs – Server, ACE, Console Station, Flex Station
ESVT – Server A	• Dell PowerEdge R710 server • (8) Processors: Intel(R) Xeon(R) CPU E5620 @ 2.40GHz • Speed: 2,394 • 12 GB RAM	4.8% – 8.9%	1 minute 40 seconds to 2 minutes 56 seconds	
EST	• Dell Precision T5500 workstation • (4) Processors: Intel(R) Xeon(R) CPU X5570 @ 2.93GHz • Speed: 2,926 • 3 GB RAM	2.7% – 6.5%	1 minute 23 seconds to 2 minutes 50 seconds	
Flex	• VMware virtual platform • (2) Processors: Intel(R) Xeon(R) CPU X5570 @ 2.67 GHz • Speed: 2,666 • 2 GB RAM	7.2% - 11.9%	4 minutes to 4 minutes 21 seconds	
ACE-T	• Dell PowerEdge T610 server • (8) Processors: Intel(R) Xeon(R) CPU X5560 @ 2.80GHz • Speed: 2,794 • 4 GB RAM	0.3% - 1.8%	1 minute 6 seconds to 3 minutes 27 seconds	

The System Inventory Tool and portal are available via www.honeywellprocess.com/support.

https://www.honeywellprocess.com/library/marketing/notes/System-Inventory-Tool-Is-it-safe-for-my-control-system.pdf

New Product Introduction: Preventative Maintenance Data Collector

Do you have a maintenance agreement with Honeywell? Then this message is for you!

Introducing the new automated Preventative Maintenance Data Collector.

The Preventative Maintenance (PM) Data Collector automates the traditionally manual activity of checking and documenting system status (preventive maintenance) information.

By automating the pass/fail preventive maintenance checks, customers can now run these checks without any assistance or on-site personnel from Honeywell.

How Does it Work?

The application automates the collection of PM data and creates an encrypted output file which is then emailed to Honeywell for analysis and output file generation. See Installation and User's Guide included with the software for more details.

Which Assets are Supported?

The PM Data Collector will support C200, C300 FIM, servers, workstations, AM, HM, HPM, NIM, LCN, and UCN assets and systems.

How Do I Obtain the Software?

Please contact your account manager for details.

What is the Output?

The output, which consists of two spreadsheets and some output files containing system audit and diagnostic data, includes system performance parameters as well as patch and installed application information.

One spreadsheet will contain raw parameter data, and the other will include disposition of the PM tasks which can be determined automatically.

These are encrypted and packaged into an output file. Once created, the output file is emailed to Honeywell for processing.

What is Included with the Software?

The .zip file contains the Software Change Notification, an Installation and User's Guide, and a Service Note. The Service Note outlines the process to be followed to collect and submit the data files.

File	Purpose
Setup.exe	PM Data Collector installation package
PM Data Collector – Installation and Users Guide.pdf	Installation and User's Guide; must read to install properly
PM Data Collector – SCN	Software Change Notice – Details about the program, known issues and any PM tasks not supported today

Products Revisions and Support Status

Latest Media Revision	Latest Patch/Update	Functional Release – First Shipment Announcement	Support Status	Software Product Category
Alarm Configuration Manager R321	R321.12	2013-10	Supported	Standalone Software
Alarm Event Analysis R321	R321.5	2013-10	Supported	Standalone Software
Blending and Movement Automation R430.y	R430.4	2014-06	Supported	Software Package
Control Performance Monitor R56x	R560.1	2013-03	Supported	Standalone Software
Control Performance Monitor R57x	R570.1	2014-12	Current	Standalone Software
Control Performance Monitor R60x	R601.2	2018-05	Current	Standalone Software
ControlEdge 2020 R14x	R140.1	2017-04	Supported	Standalone Software
ControlEdge 2020 R15x	R151.1	2018-11	Supported	Standalone Software
ControlEdge 2020 R16x	R160.2	2019-12	Supported	Standalone Software
ControlEdge 2020 R16x	R161.1	2020-04	Current	Standalone Software
ControlEdge HC900 R60x	R600.1	2014-04	Supported	Standalone Software
ControlEdge HC900 R62x	R620.1	2016-09	Supported	Standalone Software
ControlEdge HC900 R63x	R630	2017-04	Supported	Standalone Software
ControlEdge HC900 R65x	R650	2018-06	Supported	Standalone Software
ControlEdge HC900 R66x	R660.2	2018-12	Supported	Standalone Software
ControlEdge HC900 R70x	R700	2019-12	Current	Standalone Software
ControlEdge PLC R15x	R151.1	2018-11	Supported	Standalone Software
ControlEdge PLC R15x	R152.1	2019-04	Supported	Standalone Software
ControlEdge PLC R16x	R160.2	2019-12	Supported	Standalone Software
ControlEdge PLC R16x	R161.1	2020-04	Current	Standalone Software
DynAMo Alerts & Notifications (A&N) R200	UA R321.2	2013-10	Supported	Standalone Software
DynAMo Documentation & Enforcement (D&E) R200	ACM R321.12	2016-05	Supported	Standalone Software
DynAMo Metrics & Reporting (M&R) R200	R202.1	2017-03	Supported	Standalone Software
DynAMo Operations Logbook (DOL) R211	R211.4	2017-08	Supported	Standalone Software
DynAMo Operations Logbook (DOL) R220	R220.3	2018-06	Supported	Standalone Software
DynAMo Operations Logbook (DOL) R230	R230.1	2019-04	Supported	Standalone Software
DynAMo Operations Logbook (DOL) R230	R230.2	2019-08	Current	Standalone Software
DynAMo Operations Monitoring (DOM) R211	R211.4	2017-08	Supported	Standalone Software
DynAMo Operations Monitoring (DOM) R220	R220.3	2018-06	Supported	Standalone Software
DynAMo Operations Monitoring (DOM) R230	R230.1	2019-04	Supported	Standalone Software
DynAMo Operations Monitoring (DOM) R230	R230.2	2019-08	Current	Standalone Software
Experion Backup and Restore R50x	R500.1	2017-04	Supported	Software Package
Experion Backup and Restore R50x	R501.1	2017-04	Supported	Software Package
Experion Backup and Restore R50x	R501.2	2017-04	Supported	Software Package
Experion Backup and Restore R50x	R501.3	2017-04	Current	Software Package
Experion HS R41x	R410.1	2013-07	Supported	System Software
Experion HS R43x	R430.1	2015-03	Supported	System Software
Experion HS R50x	R500.3	2017-08	Supported	System Software
Experion HS R51x	R510.2	2018-09	Supported	System Software

Experion HS R51x	R511.1	2018-09	Current	System Software
Experion LS R30x	R300.1	2009-11	Supported	System Software
Experion LS R40x	R400.1	2011-06	Current	System Software
Experion LX R11x	R110.2	2014-09	Supported	System Software
Experion LX R12x	R120.1	2015-03	Supported	System Software
Experion LX R50x	R500.2	2017-11	Supported	System Software
Experion LX R51x	R510.2	2018-11	Current	System Software
Experion MX CD Controls R70x	R700.1	2017-03	Supported	Software Package
Experion MX CD Controls R70x	R701.2	2018-05	Supported	Software Package
Experion MX CD Controls R70x	R702.1	2019-06	Current	Software Package
Experion MX CDMV Controls R70x	R700.1	2017-03	Supported	Software Package
Experion MX CDMV Controls R70x	R701.1	2018-05	Supported	Software Package
Experion MX CDMV Controls R70x	R702.1	2019-06	Current	Software Package
Experion MX MD Controls R70x	R700.1	2017-03	Supported	Software Package
Experion MX MD Controls R70x	R701.1	2018-05	Supported	Software Package
Experion MX MD Controls R70x	R702.1	2019-06	Current	Software Package
Experion MX MDMV Controls R70x	R700.1	2017-03	Supported	Software Package
Experion MX MDMV Controls R70x	R701.3	2018-05	Supported	Software Package
Experion MX MDMV Controls R70x	R702.1	2019-06	Current	Software Package
Experion MX/MXProLine R70x	R700.4	2017-03	Supported	System Software
Experion MX/MXProLine R70x	R701.3	2018-05	Supported	System Software
Experion MX/MXProLine R70x	R702.2	2019-06	Current	System Software
Experion PKS R43x	R431.4	2014-03	Supported	System Software
Experion PKS R43x	R431.5	2014-03	Supported	System Software
Experion PKS R43x	R432.1	2014-03	Supported	System Software
Experion PKS R43x	R432.2	2014-03	Supported	System Software
Experion PKS R50x	R501.4	2017-01	Supported	System Software
Experion PKS R50x	R501.6	2017-01	Supported	System Software
Experion PKS R51x	R510.1	2018-08	Supported	System Software
Experion PKS R51x	R510.2	2018-08	Supported	System Software
Experion PKS R51x	R511.1	2018-08	Supported	System Software
Experion PKS R51x	R511.2	2018-08	Current	System Software
Fail Safe Controller R71x	R710.9	2011-07	Supported	System Software
Fail Safe Controller R80x	R801.3	2014-10	Current	System Software
Field Device Manager R50x	R500.1	2017-03	Supported	Standalone Software
Field Device Manager R50x	R501.4	2017-03	Supported	Standalone Software
Field Device Manager R51x	R511.1	2019-09	Current	Standalone Software
Honeywell Trace R121	R121.1	2018-01	Supported	Standalone Software
Honeywell Trace R130	R130.1 Patch 2	2019-03	Supported	Standalone Software
Honeywell Trace R140	R140.1	2020-06	Current	Standalone Software
Immersive Competency	R100.1	2018-07	Current	Standalone Software
Integrated Automation Assessment R15x	R150.1	2018-02	Supported	Standalone Software
Integrated Automation Assessment R16x	R160.1	2019-12	Current	Standalone Software
Intuition Executive R22x	R220.1	2014-05	Supported	Standalone Software
Intuition Executive R23x	R230.1	2015-07	Supported	Standalone Software

Intuition KPI R11x	R110.1	2014-05	Supported	Standalone Software
OptiVision R54x	R541.1	2012-01	Supported	Software Package
OptiVision R56x	R560.2	2014-08	Supported	Software Package
OptiVision R600x	R600.1	2019-10	Current	Software Package
PlantCruise R10x	R100.3	2013-07	Supported	System Software
PlantCruise R11x	R110.2	2014-09	Supported	System Software
PlantCruise R12x	R120.1	2015-03	Supported	System Software
PlantCruise R50x	R500.1	2017-11	Supported	System Software
PlantCruise R51x	R510.2	2018-11	Current	System Software
PMD R90x	R900.2	2017-02	Supported	System Software
PMD R91x	R910.2	2018-12	Supported	System Software
PMD R91x	R910.3	2020-05	Current	System Software
Predict-Amine	R4.0	2017-09	Supported	Standalone Software
Predict-Crude	R2.0	2015-09	Supported	Standalone Software
Predict-O&G	R7.1	2018-09	Supported	Standalone Software
Predict-Pipe	R5.0	2018-12	Supported	Standalone Software
Predict-RT	R140	2019-06	Supported	Standalone Software
Predict-SA	R2.0	2014-12	Supported	Standalone Software
Predict-SW (Sour Water)	R4.0	2018-12	Supported	Standalone Software
Procedure Analyst R41x	R410.0	2013-01	Supported	Standalone Software
Procedure Analyst R43x	R430.1	2015-06	Supported	Standalone Software
Procedure Analyst R50x	R500.2	2017-03	Current	Standalone Software
Process Safety Analyzer	R115	2017-06	Current	Standalone Software
Profit Blending and Movement R431.y	R431.4	2015-06	Supported	Software Package
Profit Blending and Movement R500.y	R500.2	2016-11	Supported	Software Package
Profit Blending and Movement R501.y	R501.3	2018-05	Supported	Software Package
Profit Blending and Movement R510.y	R510.2	2019-09	Current	Software Package
Profit Suit R41x	R411.1	2013-05	Supported	Standalone Software
Profit Suit R43x	R431.1	2014-12	Supported	Standalone Software
Profit Suit R44x	R441.1	2017-04	Supported	Standalone Software
Profit Suit R50x	R500.1	2018-10	Current	Standalone Software
Quality OptiMiser R540x	R540.1	2010-10	Supported	Standalone Software
Quality OptiMiser R550x	R550.1	2014-12	Supported	Standalone Software
Quality OptiMiser R560x	R560.1	2017-11	Current	Standalone Software
Risk Manager R170	R170.1 Patch 3	2018-03	Supported	Standalone Software
Risk Manager R171	R171.1	2019-03	Current	Standalone Software
RTU2020 R11x	R110.1	2015-06	Supported	Standalone Software
RTU2020 R12x	R120.1	2016-05	Supported	Standalone Software
Safety Historian R20x	R201.1	2014-03	Current	System Software
Safety Manager R14x	R146.2	2010-05	Supported	System Software
Safety Manager R15x	R153.7	2012-04	Supported	System Software
Safety Manager R15x	R154.2	2012-04	Supported	System Software
Safety Manager R16x	R162.4	2014-10	Current	System Software
Safety Manager SC R20x	R201.2	2018-08	Supported	System Software
Safety Manager SC R21x	R210.1	2020-06	Current	System Software

Secure Media Exchange (SMX)	104.6	2017-08	Current	Standalone Software
Socrates	R10.0	2019-03	Supported	Standalone Software
Symphonite Integration and Analytics R200.1	R200.2	2017-07	Supported	Standalone Software
Symphonite Integration and Analytics R201.2	R201.2	2020-01	Current	Standalone Software
Symphonite Production Accounting & Reconciliation	R200.1	2015-08	Supported	Standalone Software
Symphonite Production Accounting & Reconciliation	R201.2	2015-08	Supported	Standalone Software
Symphonite Production Accounting & Reconciliation	R210.1	2019-02	Current	Standalone Software
Symphonite RPMS	R510.1.8	2018-12	Supported	Standalone Software
System Inventory Tool R22x	R220.1	2017-09	Supported	Standalone Software
System Inventory Tool R23x	R230.1	2018-05	Supported	Standalone Software
System Inventory Tool R23x	R230.2	2018-05	Supported	Standalone Software
System Inventory Tool R23x	R230.3	2018-05	Supported	Standalone Software
System Inventory Tool R30x	R300.1	2019-09	Current	Standalone Software
System Performance Analyzer R120	R120.1	2019-01	Supported	Standalone Software
System Performance Analyzer R130	R130.1	2020-06	Current	Standalone Software
TPN (AM) CLM R36x	R360.12	2002-01	Supported	System Software
TPN R685.x	R685.4	2016-06	Supported	System Software
TPN R686.x	R686.4	2016-10	Supported	System Software
TPN R687.x	R687.4	2018-02	Supported	System Software
TPN R687.x	R687.5	2018-02	Supported	System Software
TPN R687.x	R687.6	2018-02	Supported	System Software
TPN R688.x	R688.2	2019-01	Supported	System Software
TPN R688.x	R688.3	2019-01	Supported	System Software
TPN R688.x	R688.4	2019-01	Current	System Software
TPS (APP) CLM R20x	R200.2	2012-07	Supported	System Software
TPS Builder R43x	R430.1	2016-05	Supported	Software Package
Uniformance Asset Sentinel R51x	R510.1	2017-04	Supported	Standalone Software
Uniformance Asset Sentinel R51x	R511.2	2017-10	Supported	Standalone Software
Uniformance Asset Sentinel R52x	R520.1	2018-12	Supported	Standalone Software
Uniformance Asset Sentinel R52x	R520.2	2019-07	Current	Standalone Software
Uniformance Executive R31x	R311.1	2018-03	Supported	Standalone Software
Uniformance Executive R32x	R320.1	2018-09	Current	Standalone Software
Uniformance Insight R11x	R110.1	2017-10	Supported	Standalone Software
Uniformance Insight R20x	R200.1	2018-06	Supported	Standalone Software
Uniformance Insight R21x	R210.1	2015-08	Current	Standalone Software
Uniformance KPI R12x	R121.1	2017-05	Supported	Standalone Software
Uniformance KPI R13x	R130.1	2018-03	Current	Standalone Software
Uniformance PHD R32x	R321.1	2015-03	Supported	Standalone Software
Uniformance PHD R34x	R340.1	2017-10	Supported	Standalone Software
Uniformance PHD R40x	R400.1	2019-06	Current	Standalone Software
Uniformance Process Studio R32x	R322.2	2016-09	Supported	Standalone Software
Uniformance Process Studio R32x	R323.1	2020-04	Current	Standalone Software
UniSim Competency Suite	R460.1	2018-04	Supported	Standalone Software
UniSim Competency Suite	R461.1	2019-01	Supported	Standalone Software

UniSim Competency Suite	R470.1	2020-01	Current	Standalone Software
UniSim Design	R460	2018-01	Supported	Standalone Software
UniSim Design	R461.1	2019-04	Supported	Standalone Software
UniSim Design	R470	2019-10	Current	Standalone Software
UserAlert R321	R321.2	2013-10	Supported	Standalone Software
Web Order Services 54x	R540.1	2014-08	Current	Standalone Software

Note: Software releases not listed in the table are in "Phased Out" lifecycle status. The HPS Product Support Guide for Control, Safety and Monitoring Systems is available for download [here](#).

Only Latest and Latest-1 patches/updates are supported by GTAC at the defined support level for the software functional release.

Definitions:

"Software Package" means any HPS software product developed for the specific functional release of system software.

"Standalone Software" means any HPS software product developed for independent operation from a system software functional release.

"System Software" means machine-readable data and executable programs used to define the functionality of the HPS control system and standard hardware products, but does not include firmware, operating system, application software or other software products.