Content Type	Support Article
Article #	000032382
Title	New Accounts and Security Groups in Wonderware System Platform 2017 Update 3 and later
Legacy DocId	TN10225
Confidence	Expert Reviewed
Published On	4/9/2024

New Accounts and Security Groups in Wonderware System Platform 2017 Update 3 and later

PROBLEM

Title

New Accounts and Security Groups in Wonderware System Platform 2017 Update 3 and later

SOLUTION

Summary

As part of the improvements made in **System Platform 2017 Update 3** and **later**, changes were made to the user accounts and groups established, which are now used by System Platform products. These accounts and groups are needed for Wonderware products to function properly. Some customers have policies to eliminate unrecognized user accounts and groups. This *Tech Note* explains some of the changes related to System Platform 2017 Update 3 and later, in order to help customers avoid problems, and to keep their systems as secure as possible.

Note: Users and Groups seen on a newly-installed **System Platform 2017 Update 3 and later** system will appear different than they will on an upgrade from a prior version. This was done to prevent upgrade problems, because customers may have developed systems reliant on those users and groups for their own purposes outside of System Platform products.

Affected Versions:

- **System Platform 2017 Update 3 (All Products)**
- **System Platform 2020 (Some Products)**
- **System Platform 2020 R2 (Some Products)**
- **System Platform 2020 R2 SP1 (Some Products)**
- **System Platform 2023 (Some Products)**

Situation

AVEVA Software takes the security of our products and customers very seriously and makes regular product security improvements. **System Platform 2017 Update 3 and later** introduces a number of security improvements designed to reduce application privileges, and to provide more granular control of user permissions.

User Accounts and Groups created and used by System Platform

APPLICATION SERVER

Application Server has the following user groups:

User Group	Description
aaConfigTools	Provides permissions to users to connect to a Galaxy from the IDE.

Application Server has the following User accounts:

User account	Description
aaGalaxyOwner	This account is the owner (dbo) of all Galaxy databases in your system.

For more information on aaGalaxyOwner, refer to **Chapter 2: Security and Permissions** of the WSP_Install_Guide.pdf.

Application Server has the following Service accounts:

Service Account	Description
NT SERVICE\aaPIM	aaPIM is platform installation manager that is responsible for installing platforms.

Additions in System Platform 2017 Update 3:

Group Name	User Name	WSP 2017 Update 3	Notes
Administrators	NT SERVICE\aaPIM	Newly-added windows services in U3.	In previous versions aaPIM is launched on demand as a process with Admin privilege but now it is changed into a windows service and added to the Administrators group as a service account. **Do NOT remove this account from this Group and the System.**
	ArchestrA User	A fresh installation of U3 will not have this user. Only an upgraded system from U2 to U3 will have this user in this group.	If no other product other than AppServer is installed, users may remove Archestra User from this group. As with any upgrade or significant change to your system, thorough testing is recommended prior putting the system into production. Please refer to TA381 for more information.
Distributed COM Users	ArchestrA User	A fresh installation of U3 will not have this user. Only an upgraded system from U2 to U3 will have this user in this group.	If no other product other than AppServer is installed, users may remove Archestra User from this group. As with any upgrade or significant change to your system, thorough testing is recommended prior to putting the system into production. Please refer to TA381 for more information.
Performance Monitor Users	ArchestrA User	Newly-added to this group in U3.	**Do not remove.**
PSMS Administrators	ArchestrA User	Newly-added to this group in U3.	**Do not remove.**

Additions in System Platform 2023:

User Group	Description
aaRuntimeUsers	Provides permissions to users belonging to this group for performing network communication through LMX APIs. The group membership is used to authenticate clients, if the “Grant Access to NMX for all users” setting is disabled in Configurator.

INTOUCH And INTOUCH WEB CLIENT

InTouch has the following User groups:

User Group	Description
aaInTouchUsers	Only users in this user group will have access to view graphics from an application in the web browser.

InTouch has the following Service accounts:

Service Account	Description
NT SERVICE\InTouchDataService	Used by InTouch Web Client as well InTouch OMI application to access InTouch tags.
NT SERVICE\InTouchWeb	Used by InTouch Web Client to browse application graphics from a web browser.

InTouchDataService and **InTouchWeb** were added as virtual service accounts to the **ArchestrAWebHosting** group to support the HTTPS protocol for InTouch Web Client.

Additions in System Platform 2017 Update3:

Group Name	User Name	WSP 2017 Update 3	Notes
ArchestrAWebHosting	NT SERVICE\InTouchDataService	Newly-added to this group in U3.	Can be removed if not using InTouch Web Client or accessing InTouch tags from InTouch OMI.
	NT SERVICE\InTouchWeb		Can be removed if not using InTouch Web Client
ASBSolution	NT SERVICE\InTouchDataService	Newly-added to this group in U3.	Can be removed if not using InTouch Web Client or accessing InTouch tags from InTouch OMI.
	NT SERVICE\InTouchWeb		Can be removed if not using InTouch Web Client
			Can be removed if not using InTouch

Administrators	NT SERVICE\InTouchDataService	Newly-added to this group in U3.	Web Client or accessing InTouch tags from InTouch OMI.
	NT SERVICE\InTouchWeb		Can be removed if not using InTouch Web Client.

Additions in System Platform 2020:

User Group	Description
aaInTouchRWUsers	Only users in this user group will have permissions to write to external references such as Application Server attributes or InTouch tags and also Acknowledge alarms with details of the operator. Note: By default, the installation user will be added to this group. Add relevant users to this group before configuring the application.

NOTE: **NT SERVICE\InTouchWeb** was removed from all groups and was replaced with **NT SERVICE\AIGWebServer** in System Platform 2020 R2 and later.

Additions in System Platform 2020 R2:

User Group	Description
InTouchHMIOPCUAWriteUsers	Members of this group can write to the InTouch tags through OPC UA Service.

Service Account	Description
NT SERVICE\AIGWebServer	Used to run the 'AVEVA Industrial Graphics Service' which is used for the InTouch Web Client

Group Name	User Name	WSP 2020 R2	Notes
Administrators	NT SERVICE\AIGWebServer	Newly-added service account to this group in 2020 R2	Can be removed if not using InTouch Web Client.
ArchestrAWebHosting	NT SERVICE\AIGWebServer	Newly-added service account to this group in 2020 R2	Can be removed if not using InTouch Web Client.
ASBSolution	NT SERVICE\AIGWebServer	Newly-added service account to this group in 2020 R2	Can be removed if not using InTouch Web Client.

Additions in System Platform 2020 R2 SP1:

User Group	Description
InTouchHMIOPCUAWriteUsers	Members of this group can write to the InTouch tags through OPC UA Service.

Additions in System Platform 2023:

Group Name	User Name	WSP 2023	Notes
		Newly-	

Administrators	NT SERVICE\View	added service account to this group in 2023	When WindowViewer is running as a service, this virtual service account is used
	NT SERVICE\Wonderware Purge Archive	Newly-added service account to this group in 2023	When virtual account option is selected in the Purger Archive utility settings, this virtual service account is used by Purge Archive service
	NT SERVICE\New_Alarmlogger		When virtual account option is selected in the Alarm DB Logger Manager settings, this virtual service account is used by Alarm DB Logger Manager Servcie
aaAdministrators	NT SERVICE\AIGWebServer	Newly-added service account to this group in 2023	Used to run the 'AVEVA Industrial Graphics Service' which is used for the InTouch Web Client

NOTE: **NT SERVICE\AIGWebServer** was removed from Administrators group in System Platform 2023.

HISTORIAN

Prior to System Platform 2017 Update 3, Historian services ran under the Local System account which has a high-level privilege. In Update 3, these services are run under the Virtual Service Accounts with specific privileges. Virtual Service Account names will have the same name as that of the service.

Historian has the following User groups:

Group name	Description
aaAdministrators	Has read and write access for Historian Data, Batch Logon Privilege, write access to ArchestrA registry Hive and additional privileges on Runtime Database.
aaPowerUsers	Has read and write access for Historian Data and Batch Logon Privilege.
aaReplicationUsers	Can replicate the data (This is on Tier 2) and has Batch Logon Privilege.
aaUsers	Can read the Historian Data.

Historian has the following Service accounts:

Service Account	Description
NT SERVICE\aahClientAccessPoint	Service Account for Client Access Point service which is the data ingest layer.
NT SERVICE\aahSearchIndexer	Service account for Search Indexer service which indexes the tags to Historian Search.
NT SERVICE\InSQLConfiguration	Service account for Configuration service that manages the Historian Services.
NT SERVICE\InSQLEventSystem	Service account for Classic Event System service.
NT SERVICE\InSQLManualStorage	Service account for Data Import service that processes CSV file imports.
NT SERVICE\InSQLStorage	Service Account for Classic Storage Service which transforms the data from legacy IDAS service.
NT SERVICE\InSQLIndexing	Service Account for Classic Indexing service that indexes the History Blocks.
NT SERVICE\InSQLIOServer	Service account Historian IOServer that provides access to data through Suitelink.
NT SERVICE\InSQLSystemDriver	Service Account for Historian System Driver that captures data for System Tags.
NT SERVICE\aahInSight	Service Account for Historian Insight.
NT SERVICE\aahSupervisor	Service Account for the Host process for Insight Publisher.

Additions in System Platform 2017 Update 3:

Group Name	User Name	WSP 2017 Update 3	Notes
aaPowerUsers	NT SERVICE\aahSupervisor	Newly-added windows services in U3.	aahSupervisor should not be removed if InsightPublihser or Historian is installed on the system.
	NT SERVICE\aahInsight		Should not be removed if Historian is installed on the system.
ArchestrAWebHosting	NT SERVICE\aahClientAccessPoint	Newly-added to this group in U3.	Should not be removed if Historian is installed on the system.
	NT SERVICE\INSQLIOServer		
Distributed COM Users	NT SERVICE\aahSupervisor	Newly-added windows services in U3.	aahSupervisor should not be removed if InsightPublihser or Historian is installed on the system.

- The Historian services are added to the **Performance Monitor Users** to acquire the performance counter information to be Historized as system tags.
- The Historian services are added to the **Performance Log Users** to allow logging performance counters.
- MSSQLServer is the SQLServer service account added to the aaAdministrators to allow the users (who have access) to perform data insertion to Historian through SQL.
- aahClientAccessPoint is added to ArchestrAWebHosting so that it can access the PCS cert which is used for encrypting the transport.
- InSQLIOServer is added to ArchestrAWebHosting to allow Secure Suitelink communication.

Additions in System Platform 2020 R2:

Group Name	User Name	WSP 2020 R2	Notes
aaPowerUsers	NT SERVICE\InSQLIndexing	Service accounts newly-added to this group in 2020 R2	Should not be removed if Historian is installed on the system.
	NT SERVICE\InSQLIOServer		Should not be removed if Historian is installed on the system.
	NT SERVICE\InSQLSystemDriver		Should not be removed if Historian is installed on the system.

Platform Common Services (PCS)

This is the System Platform communication layer, formerly known as ASB.

PCS has the following User groups:

Group Name	Description
ASBCoreServices	This group has File System and Registry permissions required by the core services of the PCS (a.k.a ASB) Framework. Since those processes are started by the PCS.Watchdog, the only user account in this group should be the NT SERVICE\Watchdog_Service virtual service account.
ASBSolution	This group has File System and Registry permissions required by the PCS (a.k.a ASB) Framework.
ArchestrAWebHosting	Only the members of this group are allowed to listen to the shared http port (80) and HTTPS port (443) - or as configured in the PCS Configurator. The other privilege of the members of this group is that they have access to the private key of the certificate used to bind to the aforementioned HTTPS port.

PCS has five Windows services:

All of the following services need "**SeServiceLogonRight**" in the group policy.

1. Watchdog_Service
   - Runs as the high-privileged virtual service account **NT SERVICE\Watchdog_Service**.
2. AsbServiceManager
   - Runs as the low-privileged virtual service account **NT SERVICE\AsbServiceManager**.
3. ASBCertificateRenewalService
   - Runs as a local system account.
   - Normally is in **Stopped** state, and will only be triggered by the Asb.Watchdog process based on the local certificate validity.
   - The service will be stopped after the certificate is renewed.
4. AIMTokenHost
   - Runs as a virtual service account **NT SERVICE\AIMTokenHost**.
   - This Service is for AIM component, and should be running after configuring the Management Server.
5. ArchestraDataStore (ADS)
   - Runs as a virtual service account **NT SERVICE\ArchestrADataStore**.
   - This service is for the ADS component. It should always be running after installation.

PCS has the following Service accounts:

Service Account	Description
NT SERVICE\Watchdog_Service	Monitors the health of the Discovery, Configuration, Service Manager processes and starts/stops them as necessary.
NT SERVICE\AsbServiceManager	Launches deployed services on the local machine.
NT SERVICE\AIMTokenHost	PCS.IdentityManager.Host (the AIM server) is running in the context of this virtual service account.

Additions in System Platform 2017 Update 3:

Group Name	User Name	WSP 2017 Update 3	Notes
ArchestrAWebHosting	NT SERVICE\AIMTokenHost NT SERVICE\AsbServiceManager NT SERVICE\Watchdog_Service	Newly-added Windows services in U3.	All processes which need access to the private key of certificates should be part of the ArchestrAWebHosting user group. PCS is a common component. DO NOT remove any account from this group.
			These two users are not introduced by the PCS but are part of this group to support

ASBSolution	NT SERVICE\InTouchDataService NT SERVICE\InTouchWeb	Newly-added to this group in U3.	InTouch Web Client. PCS is a common component. DO NOT remove any account from this group.
Users	NT SERVICE\AsbServiceManager	Newly-added Windows services in U3.	The legacy ASBService user is part of the Users group, and it is replaced by the NT SERVICE\AsbServiceManager since ASB 4.2. Adding the NT SERVICE\AsbServiceManager to Users group is for backward compatibility. NT SERVICE\AsbServiceManager can be removed. **Note:** A bug in in the v17.3 seems to add this account to this group. It will be fixed in the near future.

NOTE: **NT SERVICE\InTouchWeb** was removed from ASBSolution group from System Platform 2020 and later.

Additions in System Platform 2020 R2:

Group Name	User Name	WSP 2020 R2	Notes
AsbCoreServices	NT SERVICE\AIMTokenHost	Service accoutn newly-added to this group in 2020 r2.	DO NOT remove this account from this group.

Sentinel System Monitor

Sentinel System Monitor installs the following User Groups only when Sentinel Manager is installed and configured:

Group Name	Description
PSMS Administrators	Have full access to all Sentinel features
PSMS Advanced Support Engineers	Have access to Rules Management
PSMS Configurators	Have access to Settings management
PSMS Readonly Operators	Have access to view active alerts
PSMS Report Users	Have access to Sentinel reports
PSMS Support Engineers	Have access to Category/Sub-Category management, Publish Rules, Alert Management

Additions in System Platform 2017 Update 3:

Group Name	User Name	WSP 2017 Update 3	Notes
PSMS Administrators	NT SERVICE\psmsconsoleSrv	This is a Newly added group in U3. NT SERVICE\psmsconsoleSrv is newly added windows service and to this group in U3.	Can be removed if not using Sentinel, and after uninstalling Sentinel Manager.
PSMS Advanced Support Engineers		Newly-added group in U3.	Can be removed if not using Sentinel, and after uninstalling Sentinel Manager.

PSMS Configurators		Newly-added group in U3.	Can be removed if not using Sentinel, and after uninstalling Sentinel Manager.
PSMS Readonly Operators		Newly-added group in U3.	Can be removed if not using Sentinel. and after uninstalling Sentinel Manager.
PSMS Report Users		Newly-added group in U3.	Can be removed if not using Sentinel, and after uninstalling Sentinel Manager.
PSMS Support Engineers		Newly-added group in U3.	Can be removed if not using Sentinel and after uninstalling Sentinel Manager.

Note: The groups above are created when Sentinel Manager is installed. These groups won't be there if only the Sentinel agent is installed.

System Platform 2017 Update 3 Service Pack 1

ALL Sentinel Security Role groups ARE REMOVED (PSMS … Local) and are moved to SQL server.

Sentinel Services run under NT NETWORK VIRTUAL SERVICE ACCOUNTS. The NT NETWORK VIRTUAL SERVICE ACCOUNTS are members of the LOCAL ADMINISTRATORS GROUP, and are required to remain in the local administrator group for correct Sentinel operation).

Group Name	User Name	WSP 2017 Update 3 Service Pack 1	Notes
Sentinel Manager Administrators	NT SERVICE\psmsconsoleSrv	Newly-added group in Update 3 Service Pack 1.	Created when installing Sentinel Manager.
Sentinel Manager and Agent Administrators	NT SERVICE\simHostSrv	Newly-added group in Update 3 Service Pack 1.	Created when installing Sentinel Manager and Agent.
Administrators	NT SERVICE\adphostSrv	Newly-added group in Update 3 Service Pack 1.	Created when installing Sentinel Manager and Agent.

Licensing

Licensing has the following User Group in System Platform 2017 versions:

Group Name	Description
SELicMgr	Provides non-administrators permission to access License Server/License Manager on that computer.

Note: By default, there are no users in the **SELicMgr** group. This group can be deleted if the user(s) who will be accessing License Server and/or License Manager is an administrator on that computer.

SELicMgr User Group was updated to **AELicMgr** in System Platform 2020 version:

Group Name	Description
AELicMgr	Provides non-administrators permission to access License Server/License Manager/checkout utility on that computer.

Note: By default, there are no users in the **AELicMgr** group. This group can be deleted if the user(s) who will be accessing License Server and/or License Manager is an administrator on that computer.

Communication Drivers Pack (OI Servers / GDI)

The following is applicable from System Platform 2023. Standard users have read-only access to view the installed drivers and view diagnostics. Remote configuration or activation/deactivation of drivers is prohibited by any user type, even Administrators.

Group Name	User Name	WSP 2023	Notes
oiAdministrators	NT AUTHORITY/NETWORK SERVICE	Newly-added Username to this group in 2023	Provides permissions to users belonging to this group to perform the following operations on the local node: • View the runtime diagnostics of Communication Driver • Edit and View Communication Driver Configuration • Activate/ Deactivate/Reset/Enable/Disable a Communication Driver • Create Communication Driver/Clone/Remove Communication Driver instances • Access Autobuild, MQTT Browser, and MQTT Publisher. To access them, you need to either start the OCMC with elevated privilege or sign-in as OI Administrator in the OCMC.
ArchestrAWebHosting	NT AUTHORITY/NETWORK SERVICE	Newly-added Username to this group in 2023	Only the members of this group are allowed to listen to the shared http port (80) and HTTPS port (443) - or as configured in the Configurator. The other privilege of the members of this group is that they have access to the private key of the certificate used to bind to the aforementioned HTTPS port.
Administrators			Users in the local Administrators group (or via starting OCMC with elevated privilege) may perform the following operations on the local node: • View the runtime diagnostics of Communication Driver • Edit and view the configuration of Communication Driver • Activate/Deactivate/Reset/Enable/Disable Communication Driver • Create/Clone/Rename/Remove Communication Driver instances • Access Autobuild, MQTT Browser, and MQTT Publisher. To access them, you need to either start the OCMC with elevated privilege or sign-in as OI Administrator in the OCMC. Users in this group may also view the configuration and diagnostics of a Communication Driver remotely on a different node (read-only)

OCMC Logger

This was formerly known as SMC logger.

The following is applicable from System Platform 2023

Group Name	Description
aaLoggerProcess	Controls which users/process can actually log messages to the Logger.
	Controls who can modify the logger admin operations such as Configure, Log Flags and

aaLoggerManagement	Messages-Purge. These operations are avaiable in Action Menu and right-click context menu when a local or remote logger is selected in the OCMC Log Viewer. Only the user(s) that is part of this group will be able to perform those operations.

Links to additional technical articles related to security, configurations and guidance

1. Tech Note 000025122 (legacy TN2865): Antivirus Exclusions for System Platform 2017
2. Tech Note TN000032662 (legacy TN10567): Supplemental information for Security Bulletin LFSec00000135 - Reducing privileges
3. Tech Alert 000022219 (Legacy TA382): Issues related to Deployment failure of a platform in Wonderware System Platform 2017 Update 3
4. Tech Alert TA000032813: System Platform and related product issues with Microsoft Update KB5004442 - DCOM Hardening
5. Tech Note TN000032436: Managing Service Accounts with Group Policy for System Platform 2017 Update 3
6. Security Central: Microsoft Security Update Reports and Product Cyber Security Updates

Note: AVEVA Tech Support strongly recommends all customers follow industry best practices as documented in the NIST Guide to Industrial Control Systems Security.