Windchill PLM SaaS and ThingWorx Navigate SaaS Service Description

Effective starting: January 3, 2023

Your use of PTC's Windchill PLM SaaS and ThingWorx Navigate SaaS offerings are subject to the terms of the PTC Master SaaS Agreement (the **"Agreement"**) as well as the following additional terms. Any capitalized terms used but not defined below have the meanings in the Agreement. For the sake of clarity Windchill PLM SaaS does not include PTC's Windchill+ offering.

Version Support

The Service will include installation of new releases and update releases that PTC elects to apply to the Service. Customer will be responsible for updating customizations and/or integrations in order to ensure compatibility with the new release/update release.

PTC reserves the right to keep the Customer in a supported software release across the entire platform, and PTC reserves the right to install updates and perform general maintenance on the platform. Where Customer is not on a currently-released version of the software, PTC may terminate the Service or may impose additional fees (up to 30% of the annual contracted value on a per month basis) for each month of Services delivered by PTC.

For managed services customers, Customer is required to have a current and valid GOLDplus or higher support contract. Managed services support shall only apply if and for so long as Customer's underlying licenses of the software are current on PTC Support.

Extended SaaS Support Services

Extended SaaS Support Services may be purchased for customizations that Customer desires PTC to host for Customer, pursuant to the terms set forth on **Exhibit A**.

Regulated Industries

Regulated industries such as medical device manufacturing and military defense product manufacturing may have unique requirements for defining, tracking and managing access, security and changes to solution environments, and/or for FDA validation. For some offerings, PTC can support customers who must adhere to these requirements, but entitlement to this type of support must be explicitly purchased and is otherwise excluded. Additional terms applicable to PTC's Federal and Defense Add On Offering are as set forth on **Exhibit B**.

Data Export

Once the Service End Date is known, Customer can request up to two data exports: (1) prior to Service End Date an export for purposes of testing the input of that data into Customer's new system, and (2) final export at Service End Date. The Customer shall coordinate such requests with PTC. The data export includes the information required to redeploy the as-is software configuration in another environment. The file format(s) that are available for each offering are as set forth in the offering-specific sections below.

Other than as set forth above, export and snapshot of Data (e.g., for Customer's long-term retention needs) are not offered as part of the standard PTC offering. Customer may, however, contract with PTC for additional non-standard data export for additional fees.

PTC will retain Customer's Data for approximately 30 days following the last extraction after which time it will be destroyed. One copy of archived data can be provided during this 30-day period upon customer request.

For authorized Windchill data exports, the data export formats will include applicable items from the following: Database schema export, Directory LDIF export or similar user list export, Enterprise LDAP LDIF export, external file vault(s) contents.

Back Ups and Disaster Recovery

PTC maintains a comprehensive data backup policy to support Business Continuity and Disaster Recovery best practices. Full system backups are taken on a daily basis, and stored in geo-redundant locations. Production system backups are maintained for 30 days. Non-production backups are maintained for 7 days.

In the event of a wide-scale service outage, PTC will work with impacted Customers to determine if the Disaster Recovery protocol should be implemented. If needed, the Recovery Point Objective (RPO) for production systems is 24 hours, and the Recovery Time Objective (RTO) for production systems is 5 days. Non-production systems will be restored as quickly as possible after all production systems are fully restored.

Security and Data Privacy

Information about the security program for this Service is located at PTC's Trust Center.

Information about data that is collected as part of the Service is located at www.ptc.com/en/documents/policies.

Windchill PLM SaaS

Introduction

The Windchill PLM SaaS offering provides Customers with a SaaS environment that includes a comprehensive set of PLM capabilities described below and supports integration with external systems (such as ERP and CRM).

Offering Basis

- Windchill PLM SaaS is contracted on a "Monthly Active User" basis, which means how many individual users access the offering in a given month.
- There are defined types of Registered User profiles that may be purchased: **Windchill Base, Advanced or Premium**. Each profile grants the assigned User access only to the functionality entitled by that profile. Customers are required to allocate Users to license profiles within the Windchill production environment. Failure to appoint Users to appropriate license profiles may result in overage fees. Users may not be retroactively changed from one license profile to another.
- In some cases, it may be necessary for PTC to install and run certain Windchill compatible third-party software so the Service can process Data (e.g. data from certain non-Creo CAD systems, PTC Partner created applications, and/or document format translators). In such cases, for PTC to install and run such third-party software for Customer, it must be specifically agreed in the Quote and the Customer will be required to secure licenses and authorization for PTC to host such third-party software.
- PTC is not obligated to host for Customer any customization or custom applications unless specifically agreed in the Quote that PTC will host the same as ESS.
- Customer is responsible to configure their identity and access management integration and single sign on (SSO) experience using the provided PingFederate service as the central authentication server (CAS).
- The PTC SaaS Engagement Guide located at www.ptc.com/en/support/cloud-engagement-guide identifies the configurations, customizations and integrations that are permitted. Configurations, customizations and integrations that are not identified in such document are not permitted.

Data Storage Entitlements

Vault Content Data Storage: Customer is required to purchase a sufficient amount of vault storage space to cover all instances (i.e., production and non-production instances).

Database Storage: The Windchill service includes an allocation of database storage per User (up to 2GB per Author, and 1GB per Contributor, with none allocated for Viewers), measured in the aggregate across all customer environments. Consumption of database storage in excess of Customer's entitlement will be billed at the then-current list price for excess storage.

Additional Storage: Customer is required to purchase additional storage capacity for data migrations and/or system integrations.

ThingWorx Navigate SaaS

Introduction

The ThingWorx Navigate SaaS offering includes connectivity to a PTC SaaS Services PLM solution (purchased as SaaS or Managed Services) and, with additional fees, supports integration with certain external on-premises and cloud systems such as ERP and CRM (but not on-premises Windchill systems).

Offering Basis

ThingWorx Navigate SaaS is available as a standard service package with optional services that can be purchased separately. The solution includes software entitlement choices, a bundle of standard cloud service entitlements, and add-on cloud services to meet Customer specific requirements. It is sold as an expansion to the Windchill SaaS offerings. ThingWorx Navigate SaaS standard entitlement includes:

- Thingworx Navigate SaaS is contracted on the basis of Monthly Active Users, Active Daily Users, or Designated Computer.
- For each offering type (i.e., Monthly Active User, Active Daily User, Designated Computer), there are four profile types that may be assigned: Contribute, View, Connected PLM View, Connected PLM [Contribute]. Each User type grants the assigned User access only to the functionality entitled by that profile. The Contribute profile includes access to the View capabilities. Customers are required to create user profiles within the ThingWorx Navigate production environment. Failure to manage the creation and assignment of user profiles may result in unexpected consumption records and associated overage fees. PTC is not responsible for incorrectly managed users in the system.
- A single production instance and a single non-production instance
- Integration between a single ThingWorx Navigate and a single PTC SaaS managed Windchill instance for each included environment
- Storage allocation of 500 GB shared across all purchased environments
- A total of 6 Named Service Requests per year across all environments (option to purchase additional)
- Service Management engagement as described in the Service and Support terms and offered at the same level as entitled for Windchill PLM SaaS

The following limitations apply:

- ThingWorx Navigate SaaS apps may only connect to other software systems. Apps that connect to physical devices are not allowed as part of this Service.
- ThingWorx Navigate SaaS does not include Microsoft Azure Iot Hub as part of this Service.
- Connections to additional systems beyond those included as standard inclusion (specified above) are not included unless purchased separately and defined in the Quote.
- Active Daily User licenses are not allowed overages. Consumption will be limited to the contracted number of Users only.
- Customers are responsible to configure their identity and access management integration and SSO experience using the provided PingFederate service as the central authentication server.

Exhibit A Extended SaaS Support Services Terms

Introduction

The ESS Service provides for the deployment of a Customer's customizations and custom-developed integrations that communicate with the Service (collectively, "Customizations"). ESS does not include validation, modification, enhancement or repair of these Customizations.

Solution Scope

As part of ESS, PTC will provide:

- Application Customization installation
- verification that Customizations have installed

ESS does not provide for business use case verification or feature specific verification. Nor does it include troubleshooting or debugging of Customizations. PTC is not responsible for connectivity issues or downtime related to or caused by any Customizations.

Offering Basis

- ESS is contracted on a per Customization basis.
- PTC has the right to refuse any Customization. If PTC refuses a Customization, PTC will inform the Customer of the reason(s) to enable the Customer an opportunity to provide an updated release.
- It is important to note that the following items are not included as part of ESS:
  - Code changes required to resolve an issue or introduce new functionality
  - Customization changes following upgrades or maintenance releases or standard service enhancements
  - Data modifications
  - Customization development or consulting
  - Monitoring of Customizations
  - Services for Customizations not deployed within a PTC hosted application
- Upon Customer updating a Customization, PTC has the right to review the Customization to ensure it falls within the agreed scope of the existing Customization. If the Customization has expanded beyond the scope of the initial agreed upon baseline, PTC may require additional ESS fees to support the expanded scope.
- Upon upgrade of the PTC offering, Customer is responsible for upgrading any existing Customizations if there are any issues found during the upgrade process.

Solution Service Model

To utilize ESS, Customer is expected to provide the following components for each Customization.

- Source code
- Test plans, test cases and test results covering all use cases

PTC will analyze the documentation and source code for security and performance issues. PTC can refuse any Customization that is considered a risk in terms of performance, maintainability and sustainability of the solution, operation or security.

Exhibit B Federal and Defense Add On Terms

Introduction

The PTC SaaS Federal and Defense offering is for those Customers who require their solution to adhere to US Federal requirements for ITAR, ITIL, DFARs, CMMC, FedRAMP or IL2/IL4/IL5 certified service. This offering is sold in some cases as an add-on to an underlying offering (e.g., Windchill PLM SaaS). Whether sold as an add-on or as a complete offering, the standard terms of the underlying offering apply in addition to those stated here. Where discrepancies exist, the terms in this Federal and Defense offering description will supersede. The availability of specific software product versions may vary from PTCs general software support version matrix.

Solution Scope:

The Federal and Defense offering is available as a standard service package.

- Solutions hosted as part of this service are managed in accordance with the required regulations and all required upgrades and modifications will be applied as needed to maintain certified status. Depending on the nature of any changes, Customer may be required to participate in testing, adjusting and accepting these changes on a planned maintenance schedule set by PTC. Such changes may include an upgrade of PTC software in order to maintain overall solution compliance and third-party compatibility.

The following items are included in the standard offering for FedRAMP / IL2:

- PTC provided certification for FedRAMP where PTC will maintain an active FedRAMP authorization per regulations listed herein:
  - Cybersecurity Maturity Model Certification (CMMC)
  - DFARS 252.204-7008: Compliance with safeguarding covered defense information controls
  - DFARS 252.204-7012: Safeguarding covered defense information and cyber incident reporting
  - DoD Cloud Computing Security Requirements Guide V1 R 3
  - FAR 52.204-21: Basic Safeguarding of Covered Contractor Information Systems
  - Federal Information Security Management Act (FISMA)
  - Federal Risk and Authorization Management Program (FedRAMP)

- NIST SP 800-171: Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations
- NIST 800-53 r4: Security and Privacy Controls for Federal Information Systems and Organization

The following items are included in the standard offering for IL4 / IL5:

- For DoD SaaS customer environments, PTC will maintain an active Defense Information System Agency (DISA) authorization at the level appropriate to the requirement, to provide the relevant cloud computing services in accordance with the DISA Cloud Computing Security Requirements Guide (SRG) version in effect at the time and comply with the regulations listed herein:
  - DFARS 239.76: Cloud Computing
  - DODI 8510.01: Risk Management Framework (RMF) for DoD Information Technology
  - DoD Cloud Computing Security Requirements Guide V1 R 3
  - DoD Security Technical Implementation Guides (STIGs). In delivery of the service, PTC will comply with the following access restrictions:
    - Access to Controlled Unclassified Information (CUI) must be limited to U.S. Persons that have (1) a current U.S. security clearance (minimum interim SECRET clearance), or (2) have been the subject of a favorably completed National Agency Check with Inquiries (NACI), or (3) have been the subject of a favorably completed background check pursuant to a background check program submitted to Customer and approved by the Government.
    - Personnel with dual citizenship that have an active U.S. security clearance (interim Secret or higher) may be permitted access to Controlled Unclassified Information (CUI). Personnel with dual citizenship that do not have an active U.S. security clearance (interim Secret or higher) are not authorized access to CUI unless a request is submitted to Customer and approved in writing by Customer.

Offering Basis

The following terms describe PTCs commitment and governing practices for the Federal and Defense offering.

- PTC's SaaS Services business unit ("PTC SaaS Services") is a SaaS CSP and is FedRAMP Authorized at the Moderate Baseline. See FedRAMP.gov for more details about this.
- PTC SaaS Services meets all NIST 800-171 security control requirements required by DFAR 252.204-7012 and CMMC.
- PTC SaaS Services is audited annually by a FedRAMP and DoD approved third party assessment organization (3PAO) to ensure compliance with the FedRAMP Moderate Baseline and with the DISA SRG version in effect at the time.
- PTC SaaS Services will comply with the requirements of DFARS 252.204-7012(c)-(g) for cyber incident reporting, malicious software, media preservation and protection, access to additional information and equipment necessary for forensic analysis, and cyber incident damage assessment.
- PTC SaaS Services will ensure that all data hosted in the PTC FedRAMP and DoD Clouds remains in the United States, districts, territories, and outlying areas of the United States, and hence ensuring that the data remain under U.S. jurisdiction at all times.
- All PTC employees or authorized third parties in roles with access to DoD CUI categorized as critical sensitive will be U.S. Citizens and subject to a satisfactory Single Scope Background Investigation or other background investigation for high risk.
- All PTC employees or authorized third parties in roles with access to DoD CUI categorized as moderate risk positions or non-critical designations will be U.S. Citizens and subject to a National Agency Check with Law and Credit or equivalent.

The items below are responsibilities of the Customer:

- Customer is responsible for ensuring that only authorized personnel with current U.S. government security clearances or other authorizations, as required, are granted access to these Services.
- Customer is responsible for ensuring that any data held in these systems is appropriate given the nature of the Service, and PTC is not responsible for determining the appropriate access policies for Customer personnel or data. For example, without limitation, PTC's Services are not suitable for classified information or documents, and it is Customer's responsibility to ensure that such information/documents are not included in the Services.

Allowable Configurations

In addition to the allowable configuration terms defined for the relevant solution specific offering, the following applies for the Federal and Defense offerings:

Category	Capability
Configurations and actions not permitted for PLM	Customers may not be granted server level access to application environments for any reason.
	Integrations to third party applications that are not contained in a FedRAMP certified environment are not allowed.
	Customers are responsible to document and provide PTC with a validated code package that can be used to apply customizations and integrations on the secured production environment.

	The following add-on options available in the standard commercial offer are not permitted for Customers purchasing this Federal and Defense Add On Service. • Additional PTC hosted locations for Remote File Vaults (Replicas) • Additional services for sFTP Server or similar external file management. • Third party software extensions for CATIA WGM and Autodesk Inventor WGM • COGNOS for reporting • ECAD integrations & publishing • WinCOM extension for Windchill • CREO/Windchill AR Designshare