# Windchill PLM SaaS 与 ThingWorx Navigate SaaS 服务描述

您对 PTC Windchill PLM SaaS 与 ThingWorx Navigate SaaS 产品的使用应遵守《PTC SaaS 总协议》（下文简称“总协议”）以及下列附加条款的规定。本文件中已使用但未定义的任何首字母大写术语的含义参见总协议。 为明确起见，本文件特此申明：Windchill PLM SaaS 不包括 PTC 的 Windchill+产品。

**版本支持**
Windchill PLM SaaS 与 ThingWorx Navigate SaaS 服务将包括 PTC 选择适用的新版本和更新版本的安装。客户将负责更新客制化和/或集成数据，以确保与新版本/更新版本的兼容性。

PTC 保留权利，可在整个平台上为客户保存受支持的软件版本，并且 PTC 保留在平台上安装更新版本和执行常规维护的权利。如果客户不使用当前发布的软件版本，那么 PTC 可以终止服务，也可以基于 PTC 每个月提供的服务收取额外的费用（按月计算，最高收费可为年度合同金额的 30%）。

管理服务的客户需要拥有一份当前有效的 GOLDplus 或以上级别的支持合同。管理服务支持仅适用于客户的基础软件许可证在 PTC 支持服务仍然有效的情况下。

**扩展的 SaaS 支持服务**
对于希望 PTC 为其托管的客制化产品，客户可以根据附件 A 中规定的条款购买扩展的 SaaS 支持服务。

**管制行业**
医疗设备制造业和军事国防产品制造业等管制行业可能对解决方案环境的访问、安全和变更的定义、追踪和管理以及/或者 FDA 验证有着独特的要求。对于某些产品，PTC 可以为必须遵守管制行业特殊要求的客户提供支持，但客户应当明确购买此类支持的相关权利，否则将无权获得此类支持。 适用于 PTC 联邦和国防附加产品（Federal and Defense Add On Offering）的其他条款参见附件 B。

**数据导出**
一旦知悉服务结束日期，客户可以要求导出数据，至多两次：(1) 在服务结束日期之前，进行数据导出，以测试数据是否能够输入到客户的新系统；以及(2) 在服务结束日期当天，进行最终的数据导出。客户应就此类要求与 PTC 进行协调。数据导出包括在另一个环境中按原样重新部署软件配置所需的信息。但是，客户可以与 PTC 签订合同，通过支付额外费用，获得非标准数据导出服务。PTC 将在最后一次数据导出后的大约 30 天内保留客户的数据，然后对其进行销毁。在此 30 天的期限内，PTC 可以根据客户的要求提供存档数据的副本。就授权的 Windchill 数据导出而言，数据导出格式包括：数据库架构导出、目录 LDIF 导出或类似的用户列表导出、企业 LDAP LDIF 导出、外部文件电子仓库内容导出。

**备份和恢复**
我们每天都进行完整的系统备份，并将备份数据存储于异地冗余存放区。 生产系统备份数据的保存期限为 30 天。 非生产系统备份数据的保存期限为 7 天。PTC 无法通过许可产品恢复删除的单个文件。然而，根据客户要求，PTC 可从备份中进行完整的系统恢复。

**灾难恢复**

如果发生大范围的服务中断，PTC 将与受影响的客户合作，确定是否应当实施灾难恢复协议。 如有必要，生产系统的恢复点目标（RPO）为 24 个小时，生产系统的恢复时间目标（RTO）为 5 天。 非生产系统将在所有生产系统完全恢复之后尽快恢复。

**批处理**
对于基于许多用户（如注册用户、并发用户等，但不包括 Kiosk 用户）下的许可证类型，任何个人访问这些许可产品或其所含功能或数据，无论是直接访问、通过入口网站或“批处理”方式，还是间接访问许可产品或其功能或数据，均须获得许可。不允许一般或共享登录。

在不限制前述规定的情况下，未经 PTC 明确书面许可，明确禁止客户使用服务的应用程序接口提取服务中的数据（无论是直接使用或通过客户或第三方创建的应用程序使用），以用于训练、微调或创建人工智能（AI）模型，或建立数据源，如检索增强生成（RAG），无论是用于内部使用还是外部分发。如果客户获得该许可，所有利用该 AI 模型或数据源的应用程序用户必须拥有针对该服

务的注册用户许可，无论该等用户实际上是否直接访问服务（如果客户违反上述限制，PTC 将采取相应的救济措施，包括但不限于要求向该等用户分配注册用户许可）。此外，所有利用该 AI 模型或数据源的应用程序用户必须仅可使用相应服务中受 PTC 支持的 API。双方承认，服务构建数据的方式及相应的数据库是专有的。PTC 针对利用该 AI 模型或数据源的应用程序访问服务所授予的任何许可，并不影响该等数据结构及数据库的专有性质。

安全和数据隐私
有关产品服务的安全计划信息，请参见 **PTC 的** 信任中心
有关产品服务过程中收集的数据相关信息，请访问 www.ptc.com/en/documents/policies.

---

## Windchill PLM SaaS

**简介**
此产品为客户提供 SaaS PTC Windchill 环境。它包括以下所述的一组全面的 PLM 功能，并支持与外部系统（例如 ERP 和 CRM）的集成。

**产品基础**
- Windchill PLM SaaS 是以“月活跃用户”为基础签订的，即有多少个人用户在给定月份访问该产品。
- 可以购买已定义的注册用户配置文件类型：**Windchill 基础版，高级版或增强版**。每个配置文件只授予分配的用户对该配置文件授权的功能的访问权限。客户需要在 Windchill 生产环境中为许可证配置文件分配用户。未能为用户指定适当的许可证配置文件可能会导致超额收费。不得将用户从一个许可证配置文件追溯更改到另一个许可证配置文件。
- 当客户通过服务使用第三方 CAD 软件时，PTC 需要随服务一起安装并运行此类第三方 CAD 软件，以生成中性格式的可视文件。在这种情况下，对于 PTC 为客户安装和运行此类第三方软件，客户必须确保向 PTC 提供针对其许可服务器的 VPN 访问权限，以便使随服务一并运行的第三方 CAD 软件能够访问该软件的客户许可文件。客户应从第三方 CAD 供应商处获得授权，以允许 PTC 随服务一并托管此类第三方 CAD 软件。此外，客户将提供所有必要安装介质和文件，以便 PTC 能够随服务一并部署此类应用程序。对于 Creo 及其他 CAD 应用程序，客户需要根据每个 CAD 应用程序的用户数量和需发布的环境购买发布容量。
- PTC 没有义务为客户托管任何自定义或自定义应用程序，除非报价中明确约定 PTC 将与 ESS 托管相同的内容。
- 客户负责使用提供的 PingFederate 服务作为中央身份验证服务器 (CAS)，配置其身份和访问管理集成以及单点登录 (SSO) 体验。
- PTC SaaS 服务指南登载于 www.ptc.com/en/support/cloud-engagement-guide 确定了允许的配置、自定义和集成。不允许此类文件中未标识的配置、自定义和集成。

**数据存储权限**

内容库数据存储： 客户需要购买足够数量的内容库数据存储空间，以覆盖所有实例（即生产和非生产实例）。

数据库存储： Windchill 服务包括为每位用户的数据库分配（每个 Author 最多 2GB，每个 Contributor 最多 1GB，没有分配给 Viewers), 在所有的客户环境中测算总量。超出客户权限的数据库存储消耗将按照超出存储的当前标价计费。

额外存储： 客户需要为数据迁移和/或系统集成购买额外的存储容量。

---

## ThingWorx Navigate SaaS

**简介**
ThingWorx Navigate SaaS 产品包括与 PTCSaaS 服务 PLM 解决方案的连接（作为 SaaS 或托管服务购买），并在收取额外费用的情况下支持与外部本地部署和云系统（如 ERP 和 CRM）的集成（但不包括本地 Windchill 系统）。

**产品基础**

ThingWorx Navigate SaaS 可作为一个标准服务包使用，其中的可选服务可以单独购买。该解决方案包括软件权限选择，一组标准 SaaS 服务授权，以及附加 SaaS 服务以满足客户特定需求。它是作为 Windchill PLM SaaS 扩展出售的。ThingWorx Navigate SaaS 标准许可权包括：

- Thingworx Navigate SaaS 是在活跃用户、日活跃用户或者指定计算机基础上签约的。
- 对于每种产品类型（即月活跃用户，日活跃用户，指定计算机），有四种类型可被分配的注册用户配置文件：Contribute **贡献，View 查看，Connected PLM View 连接的 PLM 视图，连接的 PLM[Contribute 贡献]**。每个用户类型仅授予分配的用户对该配置文件授权的功能的访问权限。贡献配置文件包括对视图能力的访问。客户需要在 ThingWorx Navigate 生产环境中创建用户。未能管理用户的创建和分配可能会导致意外的消费记录和相关的超额费用。PTC 不对系统中不当管理的用户负责。
- 一个生产实例和一个非生产实例
- 为每个包含的环境集成单个 ThingWorx Navigate 和单个 PTCSaaS 管理的 Windchill 实例
- 在所有购买的环境中共享 500 GB 的存储分配
- 所有环境中每年总共 6 个指定服务请求（可选择购买额外服务）
- 服务和支持条款中描述的服务管理约定，与 PLM SaaS 在同等级别提供

以下限制适用：

- ThingWorx Navigate SaaS 应用程序可能只能连接到其他软件系统。不允许将连接到物理设备的应用程序作为此服务的一部分。
- ThingWorx Navigate SaaS 不将 Microsoft Azure Iot Hub 作为此服务的一部分。
- 除非单独购买并在报价单中定义，否则不包括与标准系统以外的其他系统的连接（如上文所述）。
- 日活跃用户许可证不允许超期使用。消费将仅限于签约用户数。
- 客户负责使用提供的 PingFederate 服务作为中央身份验证服务器，配置其身份和访问管理集成以及 SSO 体验。

---

**附录 A 扩展 SaaS 支持服务条款**

**简介**

ESS 服务用于部署客户的自定义和服务通信的定制开发集成（统称为“自定义”）。ESS 不包括对这些自定义的验证、修改、增强或修复。

**解决方案范围**

作为 ESS 的一部分，PTC 将提供：

- 应用程序自定义安装
- 验证是否安装了自定义项

ESS 不提供针对业务用例的验证或具体功能的验证。不包括自定义的排错或调试。PTC 不对与任何自定义相关或由任何定制引起的连接问题或停机负责。

**产品基础**

- ESS 是在自定义基础上签约的。
- PTC 有权拒绝任何自定义。如果 PTC 拒绝某个自定义，PTC 将告知客户原因，使客户有机会提供更新版本。
- 需要注意的是，以下项目不包括在 ESS 中：
  - 解决问题或引入新功能所需的代码更改
  - 升级或维护版本或标准服务增强后的自定义更改
  - 数据修改
  - 自定义开发或咨询
  - 自定义的监控
  - 未部署在 PTC 托管应用程序中的自定义服务
  - 客户更新自定义后，PTC 有权审查该自定义，以确保其符合现有自定义的约定范围。如果自定义的扩展超出了最初商定的基线范围，PTC 可能需要额外的 ESS 费用来支持扩展的范围。
  - 升级 PTC 产品后，如果在升级过程中发现任何问题，客户负责升级任何现有的自定义。

**解决方案服务模式**

为了使用 ESS，客户应为每次自定义提供以下组件。

- 源代码
- 覆盖所有用例的测试计划，测试用例和测试结果

PTC 将针对安全性和性能问题分析文档和源代码。PTC 可以拒绝任何在解决方案的性能，可维护性和可持续性，操作或安全性方面被自定义认为的风险。

---

## 附录 B　　联邦和国防产品条款

**简介**

PTCSaaS 联邦和国防产品面向那些要求其解决方案遵循美国联邦 ITAR，ITIL，DFARs，CMMC，FedRAMP 或 IL2/IL4/IL5 认证服务要求的客户。在某些情况下，该产品是作为基础产品的附加产品出售的（例如，Windchill PLM SaaS）。 无论作为附加产品或作为完整产品出售，除此处所述条款外，基础产品的标准条款均适用。如果存在差异，本联邦和国防产品说明中的条款将取而代之。特定软件产品版本的可用性可能与 PTC 通用软件支持版本不同。

**解决方案范围:**

联邦和国防产品是作为一个标准服务包提供的。

- 作为此服务的一部分进行托管的解决方案根据所需的法规进行管理，并且在必要时，可升级和修改，以保持认证状态。根据任何变更的性质，客户可能需要按照 PTC 制定的计划维护时间表参与测试，调整和接受这些变更。这样的变化可能包括升级 PTC 软件，以便保持整体解决方案的合规性和第三方兼容性。

FedRAMP/IL2 的标准产品包括以下项目：

- PTC 为 FedRAMP 提供认证，其中 PTC 将根据此处列出的法规保持有效的 FedRAMP 授权：
  - 网络安全成熟度模型认证(CMMC)
  - DFARS 252.204-7008：遵守涉密国防信息控制
  - DFARS 252.204-7012：涉密国防信息和网络事故报告
  - 美国国防部云计算安全需求指南 V1 R 3
  - FAR 52.204-21：相关承包商信息系统的基本安全保障
  - 联邦信息安全管理法案(FISMA)
  - 联邦风险及授权管理计划(FedRAMP)
  - NIST SP 800-171：保护非联邦信息系统和组织中的受控非机密信息
  - NIST 800-53 r4：联邦信息系统和组织的安全和隐私控制

IL4/IL5 的标准产品包括以下项目：

- 对于国防部的云客户环境，PTC 将保持主动国防信息系统局(DISA)的授权，其级别与要求相适应，以便根据当时有效的 DISA 云计算安全要求指南(SRG)版本提供相关的云计算服务，并遵守此处列出的规定：
  - DFARS 239.76：云计算
  - DODI 8510.01：国防部信息技术风险管理框架(RMF)
  - 美国国防部云计算安全需求指南 V1 R 3
  - 国防部安全技术实施指南(STIGs)。在提供服务时，PTCSaaS 将遵守以下访问限制：
    - 对受控非机密信息(CUI)的访问必须仅限于具备以下条件的美国人：（1）当前美国安全许可（最低限度临时秘密许可），或（2）已完成国家机构查询检查(NACI)，或（3）根据提交给客户并经政府批准的背景调查程序，已完成背景调查。
    - 具有有效美国安全许可（临时机密或更高级别）的双重国籍人员可以被允许访问受控非机密信息（CUI）。没有有效美国安全许可（临时机密或更高级别）的双重国籍人员无权访问 CUI，除非向客户提交请求并经客户书面批准。

**产品基础**

以下术语描述了 PTC 对联邦和国防产品的承诺和管理实践。

- PTC 的 SaaS 服务业务部门（“PTCSaaS 服务”）是一个 SaaS CSP，并在中等基线下获得 FedRAMP 授权。更多相关细节请访问 FedRAMP.gov。
- PTCSaaS 服务满足 DFAR 252.204-7012 和 CMMC 要求的所有 NIST 800-171 安全控制要求。
- PTCSaaS 服务每年接受 FedRAMP 和美国国防部批准的第三方评估组织（3PAO）的审核，以确保符合 FedRAMP 中等基线和当时有效的 DISA SRG 版本。
- PTCSaaS 服务将遵循 DFARS 252.204-7012（c）-（g）的要求，以进行网络事件报告，恶意软件，媒体保存和保护，访问法医分析和网络事件损害评估所需的其他信息和设备。
- PTCSaaS 服务将确保 PTC FedRAMP 和 DoD Cloud 中托管的所有数据都保留在美国，美国的各地区，领地和美国的外围地区，从而确保数据始终在美国管辖范围内。
- 有权访问被归类为关键敏感的美国国防部 CUI 的所有 PTC 雇员或授权第三方应为美国公民，并且需要接受令人满意的单一范围背景调查或其他高风险背景调查。
- 有权访问被归类为中等风险职位或非关键性职位的美国国防部 CUI 的所有 PTC 员工或授权第三方应为美国公民，并接受国家机构法律和信用调查或同等调查。

以下项目是客户的责任：

- 客户有责任确保只有获得当前美国政府安全许可或其他授权的授权人员才有权访问这些服务。
- 根据服务的性质，客户有责任确保这些系统中保存的任何数据是适当的，PTC 不负责确定客户人员或数据的适当访问策略。例如，但不限于，PTC 的服务不适用于涉密信息或文档，客户有责任确保此类信息/文档不包括在服务中。

**允许的配置**

除了为相关解决方案特定产品定义的允许配置条款外，以下内容也适用于联邦和国防产品：

| 类别 | 权限 |
|---|---|
| **PLM 不允许的配置和操作** | 可出于任何原因不授予客户对应用环境的服务器级别访问权限。 |
| | 不允许集成到未包含在FedRAMP认证环境中的第三方应用程序。 |
| | 客户有责任记录并向PTC提供经过验证的代码包，该代码包可用于在安全的生产环境中应用自定义和集成。 |
| | 购买此“联邦和国防附加服务”的客户不允许在标准商业产品中提供以下附加选项。<br>• 远程档库（副本）的其他PTC托管位置<br>• sFTP服务器或类似外部档管理的附加服务。<br>• CATIA WGM和Autodesk Inventor WGM的第三方软件扩展<br>• COGNOS报告<br>• ECAD集成与发布<br>• Windchill的WinCOM扩展<br>• Creo/Windchill AR设计共享 |