



## Windchill PLM SaaS 與 ThingWorx Navigate SaaS 服務描述

您對 PTC Windchill PLM SaaS 與 ThingWorx Navigate SaaS 產品的使用應遵守 [《PTC SaaS 總協議》](#)（下文簡稱“總協議”）以及下列附加條款的規定。本檔中已使用但未定義的任何首字母大寫術語的含義參見總協議。為明確起見，本檔特此申明：Windchill PLM SaaS 不包括 PTC 的 Windchill+ 產品。

### 版本支援

Windchill PLM SaaS 與 ThingWorx Navigate SaaS 服務將包括 PTC 選擇適用的新版本和更新版本的安裝。客戶將負責更新客制化和/或集成資料，以確保與新版本/更新版本的相容性。

PTC 保留權利，可在整個平臺上為客戶保存受支援的軟體版本，並且 PTC 保留在平臺上安裝更新版本和執行常規維護的權利。如果客戶不使用當前發佈的軟體版本，那麼 PTC 可以終止服務，也可以基於 PTC 每個月提供的服務收取額外的費用（按月計算，最高收費可為年度合同金額的 30%）。

管理服務的客戶需要擁有一份當前有效的 GOLDplus 或以上級別的支持合同。管理服務支援僅適用於客戶的基礎軟體許可證在 PTC 支援服務仍然有效的情況下。

### 擴展的 SaaS 支援服務

對於希望 PTC 為其託管的客制化產品，客戶可以根據附件 A 中規定的條款購買擴展的 SaaS 支援服務。

### 管制行業

醫療設備製造業和軍事國防產品製造業等管制行業可能對解決方案環境的訪問、安全和變更的定義、追蹤和管理以及/或者 FDA 驗證有著獨特的要求。對於某些產品，PTC 可以為必須遵守管制行業特殊要求的客戶提供支援，但客戶應當明確購買此類支援的相關權利，否則將無權獲得此類支持。適用於 PTC 聯邦和國防附加產品（Federal and Defense Add On Offering）的其他條款參見附件 B。

### 數據匯出

一旦知悉服務結束日期，客戶可以要求匯出資料，至多兩次：(1) 在服務結束日期之前，進行資料匯出，以測試資料是否能夠輸入到客戶的新系統；以及(2) 在服務結束日期當天，進行最終的資料匯出。客戶應就此類要求與 PTC 進行協調。資料匯出包括在另一個環境中按原樣重新部署軟體配置所需的資訊。但是，客戶可以與 PTC 簽訂合同，通過支付額外費用，獲得非標準資料匯出服務。PTC 將在最後一次資料匯出後的大約 30 天內保留客戶的資料，然後對其進行銷毀。在此 30 天的期限內，PTC 可以根據客戶的要求提供存檔資料的副本。就授權的 Windchill 資料匯出而言，資料匯出格式包括：資料庫架構匯出、目錄 LDIF 匯出或類似的用戶列表匯出、企業 LDAP LDIF 匯出、外部檔電子倉庫內容匯出。

### 備份和恢復

我們每天都進行完整的系統備份，並將備份資料存儲於異地冗余存放區。生產系統備份資料的保存期限為 30 天。非生產系統備份資料的保存期限為 7 天。PTC 無法通過許可產品恢復刪除的單個檔。然而，根據客戶要求，PTC 可從備份中進行完整的系統恢復。

### 災難恢復

如果發生大範圍的服務中斷，PTC 將與受影響的客戶合作，確定是否應當實施災難恢復協定。如有必要，生產系統的復原點目標（RPO）為 24 個小時，生產系統的恢復時間目標（RTO）為 5 天。非生產系統將在所有生產系統完全恢復之後儘快恢復。

### 批次處理

對於基於許多用戶（如註冊用戶、併發用戶等，但不包括 Kiosk 用戶）下的許可證類型，任何個人訪問這些許可產品或其所含功能或資料，無論是直接訪問、通過入口網站或“批次處理”方式，還是間接訪問許可產品或其功能或資料，均須獲得許可。不允許一般或共用登錄。

在不限制前述規定的情況下，未經 PTC 明確書面許可，明確禁止客戶使用服務的應用程式介面提取服務中的資料（無論是直接使用或通過客戶或協力廠商創建的應用程式使用），以用於訓練、微調或創建人工智慧（AI）模型，或建立資料來源，如檢索增強生成（RAG），無論是用於內部使用還是外部分發。如果客戶獲得該許可，所有利用該 AI 模型或資料來源的應用程式使用者必須擁有針對

該服務的註冊使用者許可，無論該等使用者實際上是否直接訪問服務（如果客戶違反上述限制，PTC 將採取相應的救濟措施，包括但不限於要求向該等用戶分配註冊用戶許可）。此外，所有利用該 AI 模型或資料來源的應用程式使用者必須僅可使用相應服務中受 PTC 支援的 API。雙方承認，服務構建資料的方式及相應的資料庫是專有的。PTC 針對利用該 AI 模型或資料來源的應用程式訪問服務所授予的任何許可，並不影響該等資料結構及資料庫的專有性質。

安全和資料隱私

有關產品服務的安全計畫資訊，請參見 PTC 的 [信任中心](#)

有關產品服務過程中收集的資料相關資訊，請訪問 [www.ptc.com/en/documents/policies](http://www.ptc.com/en/documents/policies).

---

## Windchill PLM SaaS

### 簡介

此產品為客戶提供 SaaS PTC Windchill 環境。它包括以下所述的一組全面的 PLM 功能，並支持與外部系統（例如 ERP 和 CRM）的集成。

### 產品基礎

- Windchill PLM SaaS 是以“月活躍用戶”為基礎簽訂的，即有多少個人用戶在給定月份訪問該產品。
- 可以購買已定義的註冊用戶配置文件類型：**Windchill 基礎版，高級版或增強版**。每個配置文件只授予分配的用戶對該配置文件授權的功能的訪問權限。客戶需要在 Windchill 生產環境中為許可證配置文件分配用戶。未為用戶指定適當的許可證配置文件可能會導致超額收費。不得將用戶從一個許可證配置文件追溯更改到另一個許可證配置文件。
- 當客戶通過服務使用協力廠商 CAD 軟體時，PTC 需要隨服務一起安裝並運行此類協力廠商 CAD 軟體，以生成中性格式的可視檔。在這種情況下，對於 PTC 為客戶安裝和運行此類協力廠商軟體，客戶必須確保向 PTC 提供針對其許可證服务器的 VPN 存取權限，以便使隨服務一併運行的協力廠商 CAD 軟體能夠訪問該軟體的客戶許可檔。客戶應從協力廠商 CAD 供應商處獲得授權，以允許 PTC 隨服務一併託管此類協力廠商 CAD 軟體。此外，客戶將提供所有必要安裝介質和檔，以便 PTC 能夠隨服務一併部署此類應用程式。對於 Creo 及其他 CAD 應用程式，客戶需要根據每個 CAD 應用程式的使用者數量和需發佈的環境購買發佈容量。
- PTC 沒有義務為客戶託管任何自訂或自訂應用程式，除非報價中明確約定 PTC 將與 ESS 託管相同的內容。
- 客戶負責使用提供的 PingFederate 服務作為中央身份驗證服务器 (CAS)，配置其身份和訪問管理集成以及單點登錄 (SSO) 體驗。
- PTC SaaS 服務指南登載於 [www.ptc.com/en/support/cloud-engagement-guide](http://www.ptc.com/en/support/cloud-engagement-guide) 確定了允許的配置、自訂和集成。不允許此類文件中未標識的配置、自訂和集成。

### 資料存儲許可權

內容庫資料存儲：客戶需要購買足夠數量的內容庫資料存儲空間，以覆蓋所有實例（即生產和非生產實例）。

資料庫存儲：Windchill 服務包括為每位元使用者的資料庫分配（每個 Author 最多 2GB，每個 Contributor 最多 1GB，沒有分配給 Viewers），在所有的客戶環境中測算總量。超出客戶許可權的資料庫存儲消耗將按照超出存儲的當前標價計費。

額外存儲：客戶需要為資料移轉和/或系統集成購買額外的存儲容量。

---

## ThingWorx Navigate SaaS

### 簡介

ThingWorx Navigate SaaS 產品包括與 PTC SaaS 服務 PLM 解決方案的連接（作為 SaaS 或託管服務購買），並在收取額外費用的情況下支援與外部本地部署和雲系統（如 ERP 和 CRM）的集成（但不包括本地 Windchill 系統）。

## 產品基礎

ThingWorx Navigate SaaS 可作為一個標準服務包使用，其中的可選服務可以單獨購買。該解決方案包括軟體許可權選擇，一組標準 SaaS 服務授權，以及附加 SaaS 服務以滿足客戶特定需求。它是作為 Windchill PLM SaaS 擴展出售的。ThingWorx Navigate SaaS 標準許可權包括：

- Thingworx Navigate SaaS 是在活躍用戶、日活躍使用者或者指定電腦基礎上簽約的。
- 對於每種產品類型（即月活躍用戶，日活躍使用者，指定電腦），有四種類型可被分配的註冊用戶配置文件：**Contribute 貢獻**，**View 查看**，**Connected PLM View 连接的 PLM 视图**，**连接的 PLM[Contribute 貢獻]**。每個用戶類型僅授予分配的用戶對該配置文件授權的功能的訪問權限。貢獻配置文件包括對视图能力的訪問。客戶需要在 ThingWorx Navigate 生產環境中創建用戶。未能管理用戶的創建和分配可能會導致意外的消費記錄和相關的超額費用。PTC 不對系統中不當管理的用戶負責。
- 一個生產實例和一個非生產實例
- 為每個包含的環境集成單個 ThingWorx Navigate 和單個 PTCSaaS 管理的 Windchill 實例
- 在所有購買的環境中共享 500 GB 的存儲分配
- 所有環境中每年總共 6 個指定服務請求（可選擇購買額外服務）
- 服務和支持條款中描述的服務管理約定，與 PLM SaaS 在同等級別提供

以下限制適用：

- ThingWorx Navigate SaaS 應用程序可能只能連接到其他軟件系統。不允許將連接到物理設備的應用程序作為此服務的一部分。
- ThingWorx Navigate SaaS 不將 Microsoft Azure Iot Hub 作為此服務的一部分。
- 除非單獨購買並在報價單中定義，否則不包括與標準系統以外的其他系統的連接（如上文所述）。
- 日活躍用戶許可證不允許超期使用。消費將僅限於簽約用戶數。
- 客戶負責使用提供的 PingFederate 服務作為中央身份驗證服務器，配置其身份和訪問管理集成以及 SSO 體驗。

---

## 附錄 A 擴展 SaaS 支援服務條款

### 簡介

ESS 服務用於部署客戶的自訂和服務通信的定制開發集成（統稱為“自訂”）。ESS 不包括對這些自訂的驗證、修改、增強或修復。

### 解決方案範圍

作為 ESS 的一部分，PTC 將提供：

- 應用程序自定義安裝
- 驗證是否安裝了自定義項

ESS 不提供針對業務用例的驗證或具體功能的驗證。不包括自訂的排錯或調試。PTC 不對與任何自訂相關或由任何定制引起的連接問題或停機負責。

### 產品基礎

- ESS 是在自定義基礎上簽約的。
- PTC 有權拒絕任何自定義。如果 PTC 拒絕某個自定義，PTC 將告知客戶原因，使客戶有機會提供更新版本。
- 需要注意的是，以下項目不包括在 ESS 中：
  - 解決問題或引入新功能所需的代碼更改
  - 升級或維護版本或標準服務增強後的自定義更改
  - 數據修改
  - 自定義開發或諮詢
  - 自定義的監控
  - 未部署在 PTC 託管應用程序中的自定義服務
  - 客戶更新自定義後，PTC 有權審查該自定義，以確保其符合現有自定義的約定範圍。如果自定義的擴展超出了最初商定的基線範圍，PTC 可能需要額外的 ESS 費用來支持擴展的範圍。
  - 升級 PTC 產品後，如果在升級過程中發現任何問題，客戶負責升級任何現有的自定義。

### 解決方案服務模式

為了使用 ESS，客戶應為每次自訂提供以下元件。

- 原始程式碼
- 覆蓋所有用例的測試計畫，測試用例和測試結果

PTC 將針對安全性和性能問題分析文檔和原始程式碼。PTC 可以拒絕任何在解決方案的性能，可維護性和可持續性，操作或安全性方面被自訂認為的風險。

---

## 附錄 B 聯邦和國防產品條款

### 簡介

PTCSaaS 聯邦和國防產品面向那些要求其解決方案遵循美國聯邦 ITAR, ITIL, DFARS, CMMC, FedRAMP 或 IL2/IL4/IL5 認證服務要求的客戶。在某些情況下，該產品是作為基礎產品的附加產品出售的（例如，Windchill PLM SaaS）。無論作為附加產品或作為完整產品出售，除此處所述條款外，基礎產品的標準條款均適用。如果存在差異，本聯邦和國防產品說明中的條款將取而代之。特定軟件產品版本的可用性可能與 PTC 通用軟件支持版本不同。

### 解決方案範圍：

聯邦和國防產品是作為一個標準服務包提供的。

- 作為此服務的一部分進行託管的解決方案根據所需的法規進行管理，並且在必要時，可升級和修改，以保持認證狀態。根據任何變更的性質，客戶可能需要按照 PTC 制定的計劃維護時間表參與測試，調整和接受這些變更。這樣的變化可能包括升級 PTC 軟件，以便保持整體解決方案的合規性和第三方兼容性。

FedRAMP/IL2 的標準產品包括以下項目：

- PTC 為 FedRAMP 提供認證，其中 PTC 將根據此處列出的法規保持有效的 FedRAMP 授權：
  - 网络安全成熟度模型認證(CMMC)
  - DFARS 252.204-7008：遵守涉密國防信息控制
  - DFARS 252.204-7012：涉密國防信息和網絡事故報告
  - 美國國防部雲計算安全需求指南 V1 R 3
  - FAR 52.204-21：相關承包商信息系統的基本安全保障
  - 聯邦信息安全法案(FISMA)
  - 聯邦風險及授權管理計劃(FedRAMP)
  - NIST SP 800-171：保護非聯邦信息系統和組織中的受控非機密信息
  - NIST 800-53 r4：聯邦信息系統和組織的安全和隱私控制

IL4/IL5 的標準產品包括以下項目：

- 對於國防部的雲客戶環境，PTC 將保持主動國防信息系統局(DISA)的授權，其級別與要求相適應，以便根據當時有效的 DISA 雲計算安全要求指南(SRG)版本提供相關的雲計算服務，並遵守此處列出的規定：
  - DFARS 239.76：雲計算
  - DODI 8510.01：國防部信息技術風險管理框架(RMF)
  - 美國國防部雲計算安全需求指南 V1 R 3
  - 國防部安全技术实施指南(STIGs)。在提供服務時，PTCSaaS 將遵守以下訪問限制：
    - 對受控非機密信息(CUI)的訪問必須僅限於具備以下條件的美国人：（1）當前美國安全許可（最低限度臨時秘密許可），或（2）已完成國家機構查詢檢查(NACI），或（3）根據提交給客戶並經政府批准的背景調查程序，已完成背景調查。
    - 具有有效美國安全許可（臨時機密或更高級別）的雙重國籍人員可以被允許訪問受控非機密信息（CUI）。沒有有效美國安全許可（臨時機密或更高級別）的雙重國籍人員無權訪問 CUI，除非向客戶提交請求並經客戶書面批准。

## 產品基礎

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。
- 根據服務的性質，客戶有責任確保這些系統中保存的任何資料是適當的，PTC 不負責確定客戶人員或資料的適當訪問策略。例如，但不限於，PTC 的服務不適用於涉密資訊或文檔，客戶有責任確保此類資訊/文檔不包括在服務中。

## 允許的配置

除了為相關解決方案特定產品定義的允許配置條款外，以下內容也適用於聯邦和國防產品：

類別	許可權
PLM 不允許的配置和操作	可出於任何原因不授予客戶對應用環境的伺服器級別存取權限。
	不允許集成到未包含在 FedRAMP 認證環境中的協力廠商應用程式。
	客戶有責任記錄並向 PTC 提供經過驗證的代碼包，該代碼包可用于在安全的生產環境中應用自訂和集成。
	購買此“聯邦和國防附加服務”的客戶不允許在標準商業產品中提供以下附加選項。
	<ul style="list-style-type: none"> <li>• 遠端檔庫（副本）的其他 PTC 託管位置</li> <li>• sFTP 伺服器或類似外部檔管理的附加服務。</li> <li>• CATIA WGM 和 Autodesk Inventor WGM 的協力廠商軟體擴展</li> <li>• COGNOS 報告</li> <li>• ECAD 集成與發佈</li> <li>• Windchill 的 WinCOM 擴展</li> <li>• Creo/Windchill AR 設計共用</li> </ul>