Ivanti 权限管理 - *技术审核员指南*

ivanti

Ivanti 权限管理 -
技术审核员指南

目录

前言

本文深入讨论了 Ivanti 应用程序管理器及其如何帮助客户在企业内达到最低权限安全状态。

关于本产品功能和高效权限管理背后的商业价值的概述和背景介绍，请参见标题为《Ivanti 权限管理》的白皮书。

Ivanti 权限管理 -
技术审核员指南

为什么需要综合权限管理

让用户对自己的电脑拥有管理员权限，就意味着他们能够接触到某些领域，这些领域一旦滥用，就可能需要耗费大量支持资源，也会影响用户体验。在很多情况下，数据丢失或恶意软件攻击都是造成安全问题的原因。

然而，在很多情况下，为了高效工作，用户的确需要获得本地管理员权限。很多应用，包括新发布的应用，都需要获得管理员权限，才能对硬件设置或网络适配器进行更改。这其中还包括网络应用升级、Acitve-X 组件安装、Adobe/Flash/Java 更新或打印机驱动安装。

为了完成这些常见任务，用户都需要获得电脑的管理员权限。Windows 7 尝试通过用户帐户控制 (UAC) 解决这个问题，但未能满足企业级管理的全部细化需求。

Ivanti 权限管理能够针对应用和控制面板程序提高或降低单个用户、群组或角色的权限级别。一个在 PC 上只有标准用户权限的用户，可以获得为他的家用打印机安装驱动的升级权限（该任务需要对机器有管理员权限）。反之，对于在 Windows 电脑上有管理员权限的用户，也可以基于防病毒设置降低其权限。

通过在用户会话的全过程中控制其权限，IT 现在可以为用户提供完成工作所需要的权限，同时保护电脑和环境，降低电脑管理成本。

Ivanti 如何实现权限管理

用户效率、安全和降低电脑拥有成本的需求三者之间的完美平衡，不是在某个会话或某个帐户级别，而是对某个应用或独立任务级别进行用户权限控制。

Ivanti 应用程序管理器通过响应用户操作，按需管理用户权限，实现动态管理应用和任务权限。另一种方式是重新采用部署本地管理员帐户的方式，最终会由于滥用、恶意软件和用户中断的频发，增加总支持成本。

针对指定应用或控制面板程序，可以为特定用户或用户组提升权限，或将某个管理员用户降为标准用户帐户权限。通过在用户会话的全过程中控制其权限，IT 现在可以为用户提供完成工作所需要的权限，同时保护电脑和环境，降低电脑管理成本。

Ivanti 在该领域提供两种处理权限管理的解决方案。

- 全功能；Ivanti 应用程序管理器在以下领域提供世界级行业解决方案：
  - 精细控制用户权限
  - 管理应用访问
  - 应用白名单和黑名单
  - 执行设备授权
  - 屏蔽不受信任的软件和代码
  - 控制网络访问
- 一套功能有限的解决方案，Ivanti 应用程序管理器 - 用户权限管理版仅包含控制用户权限的功能。

有关更多信息和特定功能的详细对比，请参见附录。

Ivanti 权限管理 -
技术审核员指南

常见场景和功能

提升应用权限

场景：为需要在标准非管理员用户电脑会话中使用升级权限运行的特定应用提升权限。本功能可用于辅助补救最低权限相关的应用兼容性场景。

优点：在本场景中，用户帐户或电脑会话不具备管理权限，但是用户可以在权限升级的情况下（不需要经过明确许可）运行需要管理员权限才可以使用的特定应用。对于那些假设所有用户都具备管理员权限（在 Windows XP 部署中的常见情况）的传统应用，本功能尤其实用。

提升控制面板程序权限

场景：许多移动用户需要安装打印机、更改网络和防火墙设置的权限，这些都需要管理员权限中的控制面板程序访问权限。

优点: 权限管理能针对单个程序升级权限，也就是让标准用户能够对他们的电脑进行必要更改，以完成工作，同时又不会获取对整台电脑的管理权限。

降低对应用和控制面板程序的用户权限

场景：指定应用或控制面板程序在降级权限下运行。用户默认具有管理权限，但任务管理器、防火墙设置或注册表编辑等特定应用必须按照非管理员用户的权限降级运行。

优点：当企业需要默认管理员权限时，例如 Windows XP 传统配置下，仍然可以保证一些系统和应用无法更改。

权限管理和互联网

Ivanti 的权限管理能力还延展到了基于网络的软件安装控制中。IT 团队现在能够可控地授权非管理用户安装和升级预先审批的网络软件，而不需要授予电脑完整管理用户权限。提升用户效率，同时将 IT 支持成本降到最低。

网站级网络安装权限

允许终端用户发起基于网络的软件安装是一种存在潜在风险的行为，即使在不授予完整管理权限时完成也一样。每存在一家合法的企业应用源，都存在无数其他提供恶意软件或未经公司批准的软件的网站，例如与效率无关或未授权的软件。

IT 管理员可以使用 Ivanti 应用程序管理器将网站加入“白名单”，让用户可以自动获得从这些网站上安装可靠软件的权限。

例如，IT 团队可以仅对知名网站授予基于网络的软件安装预授权，例如 **www.adobe.com** 和 **www.gotomeeting.com**。这样最终用户可以立即获取访问常用商务应用的权限，如 Adobe Reader、Adobe Air、Adobe Flash Player 和 GoToMeeting 或 WebEx 网络会议客户端，不会遇到 IT 应用导致的瓶颈和低效率。

受信所有权

除了允许用户群体访问 IT 未提供的个人高效应用外，安全性和完整性也得到了维护，因为用户无法从任何其他来源安装网络软件，从而降低了未授权软件安装带来的安全隐患或系统不稳定，以及相关的成本。

应用级别网络安装

尽管对于很多企业来说，网站级别的软件安装政策可能代表了安全性和简洁性之间的良好平衡，但有些企业可能需要对用户可以在某个通过审核的网站上能够安装的应用进行更精细化的控制。

回到之前的例子上，一位 IT 管理员也许希望允许安装 Adobe Reader，但是屏蔽 Adobe Air、Adobe Flash Player 和/或任何来自 www.adobe.com 的软件。在这种场景下，Ivanti 应用程序管理器为 IT 管理员提供完成上述任务所需的控制权，可以按照不同版本将制定应用加入白名单，并按照需要提供指定网站内的 ActiveX 控制级别 ID。这样就能够保证终端用户只能从网络中安装制定应用的受信任版本。

同时对在企业环境中管理应用版本控制也有帮助。

预配置网络安装权限应用模板

在提供精细化用户权限政策创建和个性化功能，应对各种复杂场景的同时，Ivanti 应用程序管理器也能大大简化常规应用政策场景，从而降低实施所需的时间。

需要为终端用户扩展网络软件安装权限的 IT 团队可以从常规企业应用的预设模板库中获得帮助。应用这些模板能够节约时间，并确保用户只会获得高效工作所需的最低权限升级。

Ivanti 应用程序管理器包含授予选中用户“自助升级”应用执行，获取升级权限的选项，同时保证权限被升级的应用依然安全，对 Windows 浏览器或任何相关会话的访问权依然保持标准用户级别，不会继承被升级应用中的管理权限。

自助升级可以由系统管理员进行配置，设定只有一批预定义列表内的授权应用可以升级，或是相反，列出禁用升级的应用，避免其被自助升级，例如 CMD.exe 或 RegEdit.exe。

受信所有权拒绝执行任何由非受信所有者（例如一个典型的用户帐户）引入的任何代码，即使是未知的。“受信所有权”的独特概念是 Ivanti 应用程序授权政策管理方法的关键元素。受信所有权提供额外的安全和控制等级，只允许执行那些被预定义的受信用户帐户“拥有”（相关）的应用。“受信所有者”的一个例子是本地系统、管理员或域管理员帐户，以及通常还会包含管理该电脑的帐户。

Ivanti 应用程序管理器的功能与现有的 Ivanti 受信所有权政策框架完全兼容。IT 管理员可以指定被批准的网络安装，如 Adobe Reader 和 GoToMeeting 可以进行自动配置，这样就可以将文件所有权分配给现有的受信所有人，而不是发起者的用户帐户。这样，即使是在管理严格的受信所有权政策下，被批准的网络安装应用也可以执行了。

Ivanti 权限管理 -
技术审核员指南

了解您现有的本地管理员情况

移除非必要的本地管理权限是很多 IT 部门的主要目标，因为这样做能够降低维护电脑环境的总成本，同时以明智的方式确保用户能够获取他们需要的应用和操作系统功能的访问权，从而保证高效。

不幸的是，如果不事先了解您现有的本地管理员情况，权限管理解决方案的实施可能会是一个漫长的过程。

然而，幸运的是，使用用户权限发现模式 (RDM)，企业可以快速掌握哪些应用和操作系统功能需要在全主机范围内升级许可，从而简化流程，加快实现。

引入用户权限发现模式

RDM 让系统管理员可以监控、分析和同步报告上万个端点，定位需要管理员权限的应用和任务。RDM 生成的报告可以按照用户、电脑或应用分组，使其中的趋势易于被发现。只需点击几下，RDM 所发现的应用和任务就可以快速加入 AM-URM 配置中。

默认/标准权限政策允许客户只需找到需要采用升级政策的目标应用，然后自动将应用分配到升级规则中，进一步简化配置，加快 AM 或 AM-URM 的实施。

表 1 是一张 RDM 报告的电脑屏幕截图，按照应用分组，管理员非常快捷地将定位到的一个需要管理权限的应用加入了全部用户的默认权限升级政策中。通过文件名也可以完成该操作，或是为了安全起见，也可以仅为该特定应用运行安全哈希算法。

注意：在截图右上角的“列表视图”中，可以看到每个应用的运行次数，以及运行的机器。本应用详细信息视图中，您可以看到该应用的每个实例的用户、机器、命令行和开始时间。

表 1 - 用户权限发现模式截图

自助权限调整

在企业环境中通常会存在一些高级用户，Ivanti 应用程序管理器为系统管理员提供了授予选定（高级）用户自助将自己的权限从他们的默认标准用户帐户升级到本地管理员的选项。这样既能使重要的用户保持高效，又降低终端用户请求相关的桌面调用支持和相关成本。

表 2– 用户权限自助升级选项

Ivanti 权限管理 -
技术审核员指南

简洁的用户体验

自助升级流程对用户极其简单，同时与 Windows 桌面无缝集成。用户只需右键点击目标应用，然后在相关菜单中选择“使用管理权限运行（已审核）”。

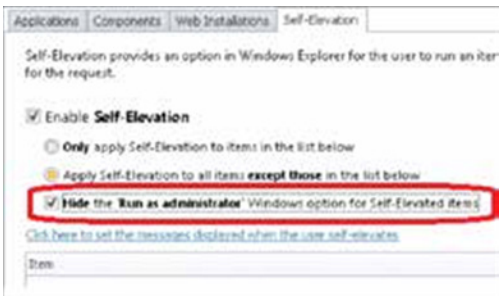

表 3 - 移除 Windows“以管理员身份运行”选项的选项

为了简化用户体验，同时确保任何自助升级都被捕捉并审核，标准 Windows 内置的“以管理员身份运行”选项也可以在右键菜单中移除，仅剩下 Ivanti 主机中的 Ivanti 自助升级选项。

自助权限调整的精细化控制

为了让系统管理员能进行精细化控制，本功能的可配置性极高，并且能根据用户、设备、位置和时间与日期动态更改配置。

自助权限调整的人物和时间

自助权限调整可以按照现存的很多 Ivanti 应用程序管理器进行授权，包括：用户名称、用户群组、设备名称和 IP 地址。这提供了一种自动根据用户、设备、位置和时间与日期的情况进行改变的动态配置功能，确保自助权限调整只会在得到系统管理员批准和指定的的时间出现。

用户可以进行自助权限调整的内容

当授予用户自助调整其权限的选项时，您可能需要限制某些应用或操作的权限。为了实现这一点，Ivanti 应用程序管理器为系统管理员提供了两个选项，可以配合使用，提供更精细化的控制：

- 白名单 - 指定用户可以自助调整权限的应用。
- 黑名单 - 指定用户不能自助调整权限的应用。

例如，系统管理员也许需要创建一个配置，其中将 Notepad.exe 加入白名单，成为授权应用，而 RegEdit.exe 加入黑名单，成为禁用应用。

自助权限调整的审计与报告

IT 支持团队经常遇到的一个问题是弄清楚“谁”和“为什么”需要管理权限。Ivanti 应用程序管理器的报告选项能够为权限发现流程提供帮助。

自我陈述

当用户选择自助调整其权限到管理员，并得到这样做的授权时，有一个选项是要求用户提供自助调整权限的理由。用户会看到一个提醒信息，其中有一个简单的文字输入框，供其输入理由。

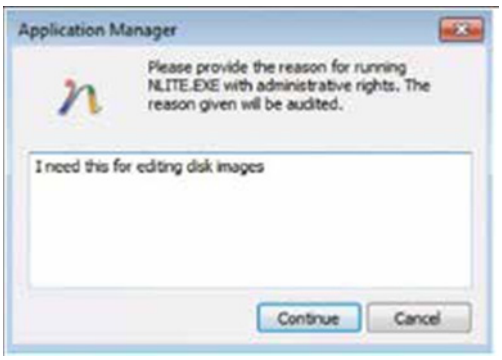

表 4 - 审计和追踪用自助权限调整陈述

中心化报告和事件日志

中心化报告和事件日志也能捕捉到自助权限调整请求的用户名称、应用名称、时间、日期，以及进行请求的机器。同时还包含用户提供的自助权限调整陈述信息。

Ivanti 权限管理 -
技术审核员指南

Ivanti 应用程序管理器和内部应用商店

Ivanti 应用程序管理器使企业能够研发自己内部的、私有的应用商店，并授权指定用户在需要时引进应用，不需要为 IT 增加负担，也无需等待请求完成。

怎么做和为什么

有关何时进程和应用应该升级、为何要升级，Ivanti 应用程序管理器为系统管理员提供了设置指定网络驱动或已知的安全位置的选项，当用户尝试从上述位置进行安装时，Ivanti 应用程序管理器将针对安装提升权限，确保电脑安全，同时让用户可以通过自助服务安装良性应用。

这不仅能通过允许自助服务改进终端用户体验，满足其自身的 IT 服务需求，同时也能降低 IT 服务成本，让 IT 能集中精力为核心业务和公司应用服务。

精细化控制

可以利用用户及用户群组规则来分部门创建应用商店，这样便能通过用户名称或其群组身份决定他们能访问哪些应用商店和安装哪些应用程序。

基于设备的规则同时也能确保在安全位置的预定义应用只能在许可（如公司）的设备上安装。

安全对话框

当应用以升级的权限发布后，必须保证该应用不会成为以管理员身份访问底层桌面、操作系统、其他应用或文件的通道。

安全对话框控制

Ivanti 应用程序管理器安全对话框控制功能确保只有应用升级到了管理员权限，其他任何对话框，如“打开文件”或“保存文件”（有可能访问计算机完全的文件结构），依然保留标准用户权限，避免其访问或更改受限文件和文件夹。

在表 5 的例子中，微软 Word 被升级到了管理员权限，但无法以管理员权限通过安全对话框进行访问。这样就避免了用户以升级后的本地管理员身份导航到操作系统的其他位置，或生成新进程。

在框内思考

安全对话框功能默认打开，保护系统和数据，避免用户恶意或意外更改文件。包括：

- 重命名或删除不属于当前用户的文件
- 将文件拖拽进出锁定目录
- 将文件复制进出锁定目录
- 更改文件的安全许可

子进程控制

与安全对话框相似，任何从升级进程或应用中产生的新进程都不继承升级权限，无论新进程是否由用户手动启动。如果允许上述情况发生，将会在应用升级后，使应用和主机有被滥用的可能，造成严重安全风险。

问题案例：某一应用升级到了管理权限，用户执行了“文件”>“打开”对话。用户浏览文件系统，找到 cmd.exe，并启动该应用。现在该应用作为升级的 Word 进程的子进程运行。

Ivanti 应用程序管理器如何解决：如果没有子进程控制，现在该应用将按照本地管理员权限运行，用户可能造成操作系统严重损坏。

Ivanti 应用程序管理器允许系统管理员防止任何子进程继承父进程的升级权限，从而避免这一安全风险。

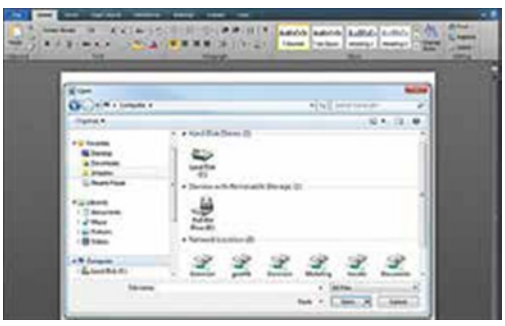

表 5 - 显示在应用内访问文件系统的对话框

Ivanti 权限管理 -
技术审核员指南

结论

在今天的很多企业中，权限管理控制不当都是一个严重的问题，会带来不必要的业务风险，并严重增加支持成本。

Gartner 的分析强调，公司通过有效控制权限，削减管理授权，最多可节约 1278* 美元。

Ivanti 应用程序管理器和 Ivanti 应用程序管理器用户权限管理版为 IT 提供更多弹性，让他们能更精细地解决访问和权限问题，而不使用一刀切的模式。

这种更强的控制最终能够降低主机管理成本、安全风险和服务请求，并提升终端用户体验和员工效率。

更多信息，请访问 **www.ivanti.com/products/desktop/ desktopnow/**

附录

工作原理：Ivanti 应用程序管理器和本地安全权限 (LSA) 令牌

在微软 Windows 运算环境中，当一个应用执行请求下达时，应用会请求一个安全令牌，作为应用运行批准进程的一部分。这些令牌包含应用的权限和许可的详细信息，这些权限可以用于与操作系统或其他应用互动。

当配置 Ivanti 应用程序管理器管理某个应用时，所请求的安全令牌会动态修改，包含升级或降级的许可，这样该应用就可以根据权限的升级或降级，开始运行（或被屏蔽）。

有些控制面板程序，包括网络适配器功能，一般会被 explorer 进程控制。将 explorer.exe 升级到可以在本地管理员环境中运行是绝对不推荐的，因为这样整个操作系统都可能遭到攻击，与最小权限的目标背道而驰。为了有效解决这一问题，使用户能够在管理员环境中访问该组件功能，Ivanti 应用程序管理器为用户提供了一个 Ivanti 生成的窗口，包括控制面板程序，可以以限定为该功能的访问级别进行控制，从而不用改变与整个桌面相关的任何权限

Ivanti 权限管理与现有安全规则无缝整合，不会创建任何新的本地管理员帐户，这些帐户之后会被引用或用于为特定应用升级权限。

Ivanti 应用程序管理器使用 detoured hook 在真正的应用（目标应用）启动前，拦截执行调用。Ivanti 应用程序管理器随后用一系列规则检查应用请求的变量，判断其是否与任何 Ivanti 应用程序管理器配置内的启用规则和政策匹配。如果匹配，Ivanti 应用程序管理器随后会为指定进程从本地安全权限中请求一个独有访问令牌。

注意：与其他解决方案不同，Ivanti 应用程序管理器不修改原始用户令牌，因此能够保证系统安全。

如今，Ivanti 应用程序管理器和定制的授权包用来自管理员分组成员安全标识 (SID) 中的管理员权限顶替新创建的独有令牌。Ivanti 应用程序管理器随后为指定进程保留原始令牌，插入新令牌，这样 Ivanti 也能够安全控制安全对话框和子进程。

Ivanti 权限管理 -
技术审核员指南

功能矩阵

以下功能矩阵列出了本文件中提及的 Ivanti 应用程序管理器的详细功能：

权限发现	
用户权限发现模式	能够识别对运营系统发出管理权限调用的现有应用
用户权限发现结果分组	按照应用、机器或用户
能够管理发现报告中的应用	快速将应用添加到配置中，从而加速实施
升级时的上下文控制	
对升级对象的上下文控制	定义单个或一组应用、控制面板程序和系统任务
升级时的上下文控制	基于用户、设备位置和时间/日期上下文的配置规则
升级位置的上下文控制	基于设备 IP 地址或应用位置的动态规则
升级设备的上下文控制	仅允许对预定义的设备进行升级
可升级对象	
应用的升级权限	为单个或一组应用创建白名单和黑名单
控制面板程序升级权限	为单个或一组控制面板程序创建白名单和黑名单
系统任务的升级权限	为单个或一组系统任务创建白名单和黑名单
降级时的上下文控制	
对降级对象的上下文控制	定义单个或一组应用、控制面板程序和系统任务
降级时的上下文控制	基于用户、设备位置和时间/日期上下文的配置规则
降级位置的上下文控制	基于设备 IP 地址或应用位置的动态规则
降级设备的上下文控制	仅允许对预定义的设备进行降级
可降级对象	
应用降级权限	为单个或一组应用创建白名单和黑名单
控制面板程序的降级权限	为单个或一组控制面板程序创建白名单和黑名单
系统设置的降级权限	为单个或一组系统任务创建白名单和黑名单
互联网控制和网络安装	
启用网站级别应用安装	指定用户可以进行安装的受信任网站
启用定义网站上的应用指定安装	在受信任网站中，指定用户可安装的授权应用
为应用安装分配受信所有权	实现与 Ivanti AppSense 受信所有权应用访问的无缝整合
提供预配置的网站模板	通过创造性的模板简化并加快实施
自助权限调整	
用户自助权限调整	启用授权用户无需 IT 服务请求即可自助调整权限
自助权限调整的用户认证	用户需要提供经核准的自助权限调整理由
自助权限调整的审计	报告提升人员、提升对象和设备
可自助调整权限人员的上下文控制	基于用户名称、分组或预设索引
可自助调整权限对象的上下文控制	自助权限调整对象的白名单或黑名单
自助权限调整时间的上下文控制	基于时间和日期，或其他上下文规则
自助权限调整地点的上下文控制	基于设备位置或应用搭载地点
自助权限调整设备的上下文控制	允许任何指定设备进行自助权限调整

Ivanti 权限管理 -
技术审核员指南

内部应用商店	
创建可作为安装来源的已知安全位置	仅允许提升从预定义位置安装的应用
额外安全控制	
能够确保会话框安全	避免被升级的应用访问底层的桌面
能够控制子进程	确保新的子进程继承升级后的权限

Ivanti 应用程序管理器和 Ivanti 应用程序管理器用户权限管理版的区别

功能	Ivanti 应用程序管理器 URM 版	Ivanti 应用程序管理器
用户权限发现模式	✓	✓
权限管理和启用的上下文控制	✓	✓
基于元数据的精细配置选项	✓	✓
网络和应用级别安装控制	✓	✓
用户自助服务和自助授权选项	✓	✓
会话框和子进程控制	✓	✓
数字签名验证控制	✓	✓
审计和报告功能	✓	✓
用户权限白名单和黑名单应用	✓	✓
应用访问白名单和黑名单应用		✓
设备证书执行		✓
动态应用访问授权		✓
屏蔽执行不受信任的代码（受信所有权）		✓
感知上下文应用终端		✓
未授权或自验证应用记录		✓
精细的 URL 过滤和重定向选项		✓
网络访问控制		✓
应用时间限制		✓
应用实例数量控制		✓
脚本、批处理文件和注册表控制		✓
用户引入可执行代码被动报告		✓
端点分析和应用使用扫描		✓
预设 Ivanti 配置模板		✓


ivanti