SafeConsole 使用手册

目录

简介

本指南为 SafeConsole 管理用户提供了日常配置和处理 SafeConsole 所需的知识。

本指南适用于 SafeConsole 云和本地部署管理员。但是，它不涵盖本地部署的内容。

有关最新的资源，请访问我们的支持页面。关于 PortBlocker 的部署，请参考 PortBlocker 管理指南。

什么是 SafeConsole?

SafeConsole 是一个 Web 服务器和数据库，经过认证的管理员可以通过 Web 浏览器来管理注册的终端设备。这些终端设备通过 HTTP SSL 连接到 SafeConsole 服务器（使用 TLS 1.2，可通过配置端口进行连接，默认端口为 443），以注册并获取其策略和配置信息。

SafeConsole 的目的是什么?

SafeConsole 为企业提供对便携式加密存储设备和终端 USB 端口的使用控制，同时支持用户进行密码重置等功能。

SafeConsole 如何管理这些设备?

终端设备使用只读分区上的独立设备软件注册到 SafeConole，注册方式如下：

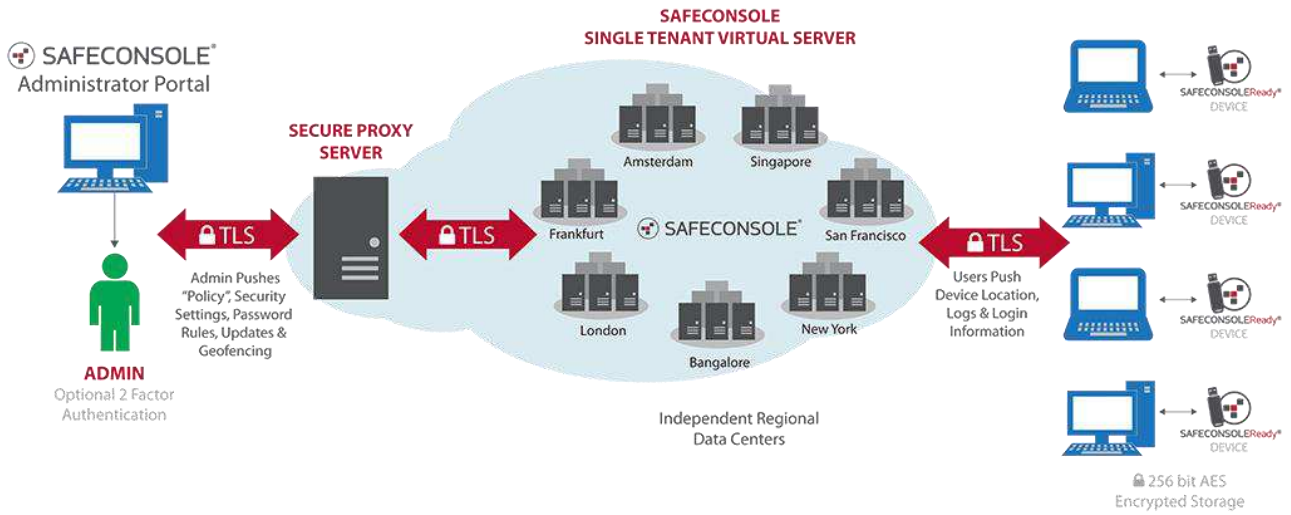
设备软件识别已部署的注册表项，其中包含 SafeConsole 连接令牌。这会提示设备软件进入设置过程，并根据注册表项的内容预先填充连接令牌。

用户在设备软件中输入服务器通用的 SafeConsole 连接令牌，可选择与随机唯一的注册令牌配对。该令牌可通过 SafeConsole 与快速连接指南一起通过电子邮件发送。

注册后，这些设备就会将服务器信息嵌入设备的隐藏区域，并可在任何计算机上使用（如果您的设备策略允许）。

如果您希望代表您的终端用户注册设备，可以在 SafeConole 中重新分配驱动器。

终端通信和设置流程对于 SafeConsoleCloud 和 SafeConsole On-Prem 是相同的。



SafeConsole 基础知识

SafeConsole 人员访问权限

可以通过不同的账户类型访问 SafeConsole Web 控制面板：

- 账户所有者：账户所有者是在导入许可证时创建的初始 SafeConsole 管理员。某些 SafeConsole 功能仅对此管理员可用，并且此管理员具有对所有设置的完全访问权限。
- SafeConsole 管理员访问是通过电子邮件地址设置的，以接收带有激活链接的邀请。该邀请还包含指向 SafeConsole 服务器的 URL。
- SSO 管理员允许通过 SAML2.0 连接将 SafeConsole 访问权限授予联合服务中的用户。
- SafeConole On-Prem 可以通过在 SafeConsole 配置程序中设置的凭据或分配给已配置安全组的 Active Directory 凭据进行访问。

SafeConsole 快速学习的最佳实践

遵循以下方法，能够高效地将 SafeConsole 解决方案部署到您的组织：

1. 仔细阅读本指南的基础知识部分。
2. 配置：尝试配置一些适用于所有设备的策略。
3. 连接：注册您的终端设备并查看策略的执行情况。
4. 管理设备：尝试执行密码重置或恢复出厂设置等操作。

5. 报告：查看并导出报告。您的组织可能会要求您回答有关系统的问题。熟悉 Excel 中导出的 XML 或 CSV 格式报告。

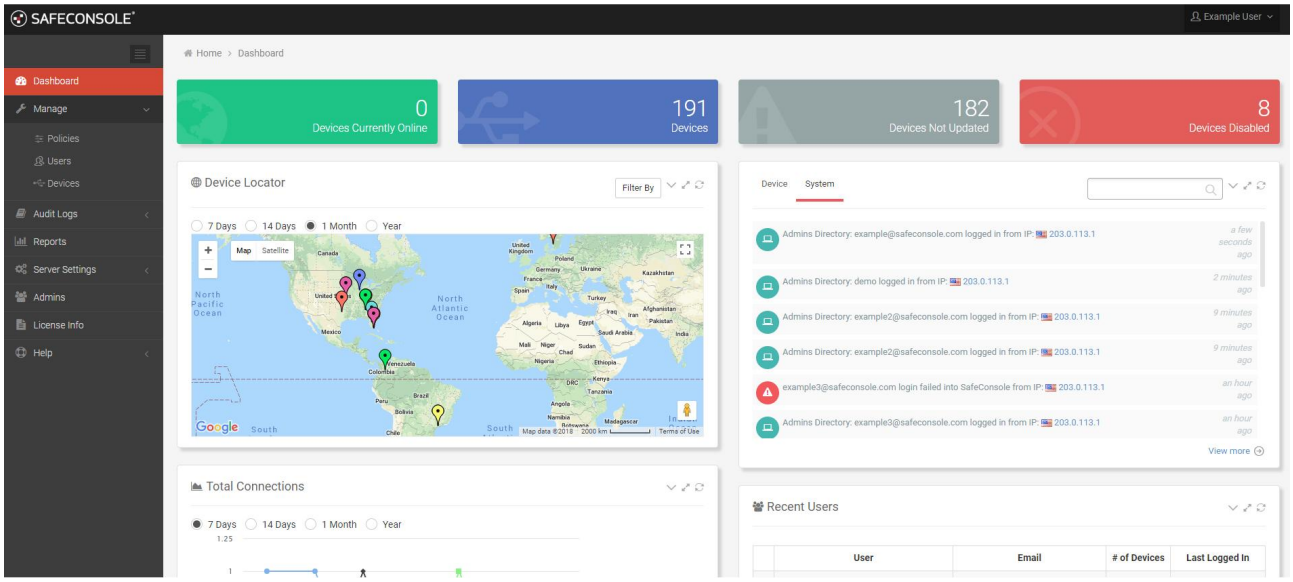
SafeConsole 界面介绍

SafeConsole 的左边有一个主菜单，右上角有一个下拉菜单，用于个人资料设置和注销。在个人资料设置中，每个 SafeConsole 工作人员都可以激活双因素身份验证。SafeConsole 管理员可以在主菜单的 Admins 选项卡下验证双因素身份验证是否已被激活。

简而言之，这些是主要的菜单项。

Dashboard 仪表板

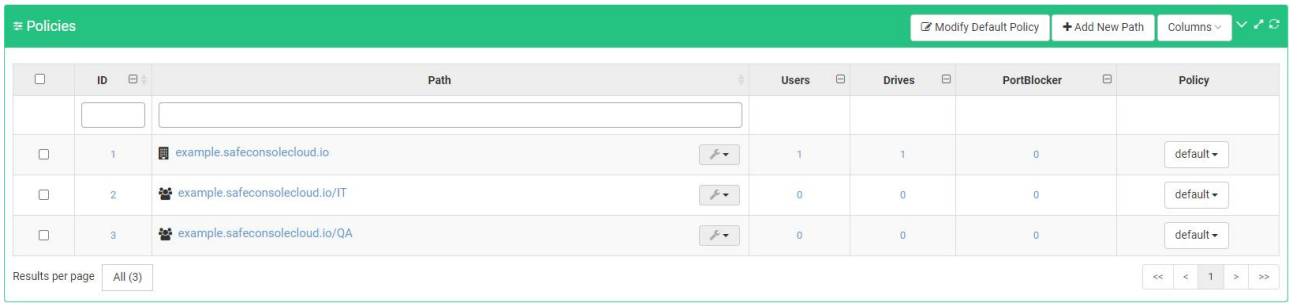
SafeConsole 的登陆页面提供了一个服务器的仪表板。



Manage 管理

SafeConsole 的管理页面可以编辑和配置策略、用户、驱动器和端点的 Portblock。在"Admin"部分，点击蓝色链接将根据所选链接过滤条目。例如，点击用户路径将显示该路径的策略，点击用户栏中的链接将显示相应的用户和该用户的设备，点击驱动器部分的所有者、用户或设备序列号将显示相关的弹出窗口。你可以使用这些过滤器来帮助寻找相关条目。

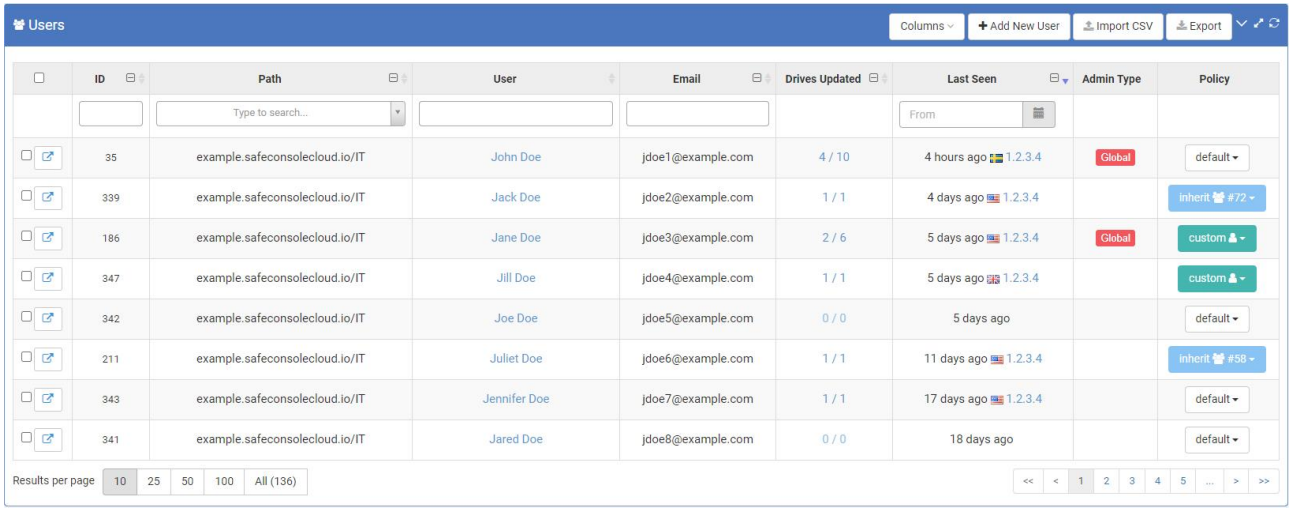
Policies 策略



根据用户的路径修改默认策略或设置已注册终端设备的配置。路径直接关系到用户在目录服务中的位置，如微软的 Active Directory。一个路径可以包含多个用户。通过选择其活动策略版本（如自定义#2），编辑路径的策略。所有的策略配置将出现在一个弹出窗口中，点击保存以应用新策略。

页面上有蓝色的内联帮助文本和更多信息图标，可以展开并解释每个策略。每次终端设备与 SafeConsole 连接时，都会进行检查和应用策略。要删除并重置所有路径、用户和设备的所有策略，请打开策略编辑器，然后点击最下面的"Danger Zone"。

User 用户

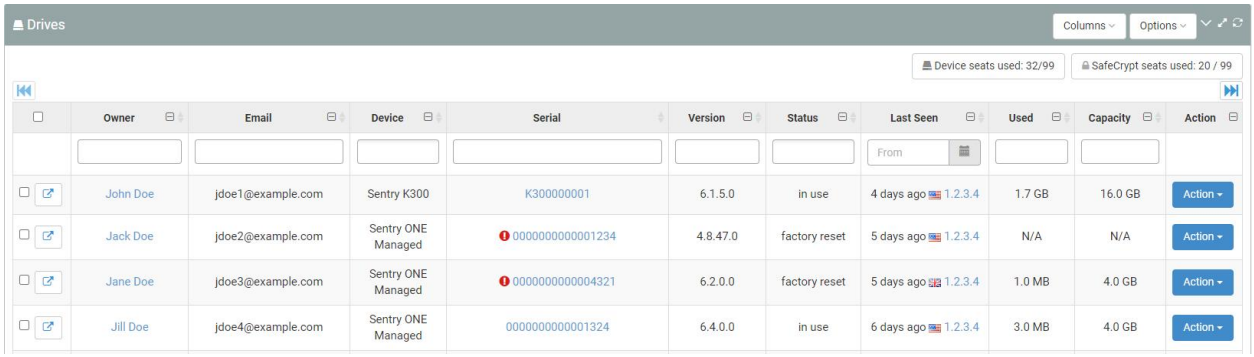


显示组织的用户。在这里，你也可以从系统中删除用户，并对他们的终端设备进行操作。点击用户栏中的蓝色链接，可显示用户详细信息窗口。在这里，可以编辑用户的姓名、电子邮件和路径。这个弹出窗口还显示了用户注册的终端设备，并提供了在电子邮件中向用户发送唯一令牌的选项。

在右上方，你可以管理要显示的列，并以 CSV 或 XML 格式导出所有注册数据。在下拉菜单中，选择你想显示或删除的数据列。点击下拉菜单外的区域以关闭它。数据将根据你的选择进行更新。为了方便滚动水平轴上的列，按住 Shift 键+鼠标滚轮。这适用于 SafeConsole 中的所有数据表。

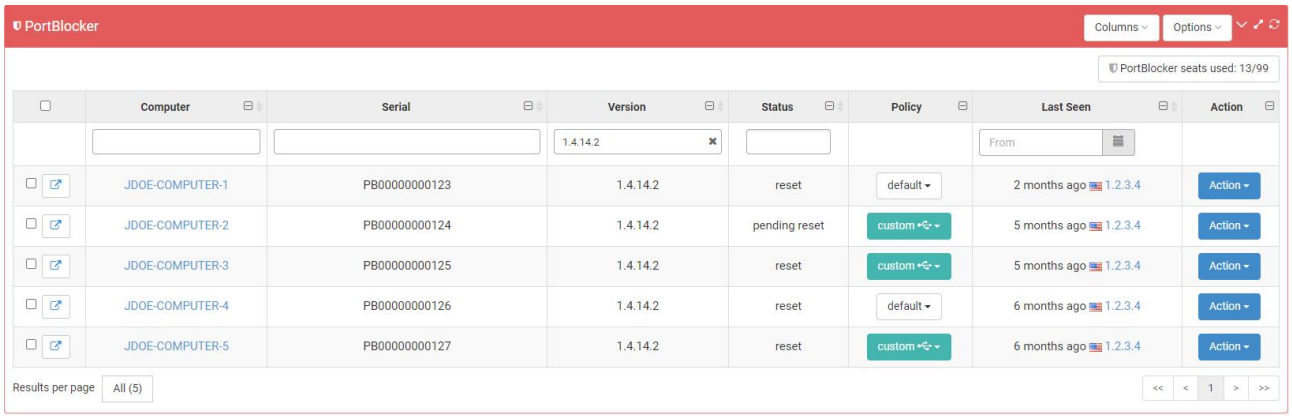
要添加用户，你可以手动逐个添加新用户，或导入标准 CSV 格式。点击"+添加新用户"按钮，可以看到屏幕截图，以逐一创建用户。导入 CSV 弹出窗口中包含了添加的说明，以辅助这一过程。

Drives 驱动器



显示所有注册的驱动器及其所有元数据，并允许你对它们执行操作。如果你点击驱动器的序列号（或左栏的弹出窗口按钮），将显示"驱动器详细信息"窗口，你可以查看和编辑设备信息。

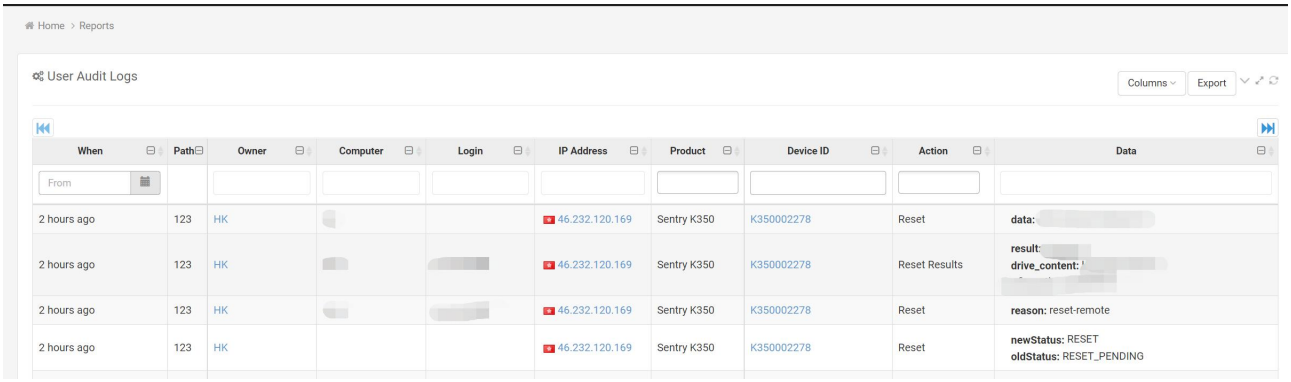
PortBlocker



显示所有注册的 Portblocker 端点及其所有元数据，并允许你对它们执行操作。如果你点击计算机名称（或左栏的弹出窗口按钮），将显示"端点详细信息"窗口，你可以查看和编辑端点信息。

Audit Logs 审计日志

审计日志包含用户审计日志和系统消息的子菜单。用户审计日志包含所有的端点操作、使用情况和文件审计（如果已激活）。系统消息显示 SafeConsole 管理人员的操作。



Report 报告

显示连接、设备库存和地理位置的三个动态报告模板。

Server Settings 服务器设置

在子菜单选项中，你可以配置设备注册、设备密码重置、SMTP、电子邮件模板、SIEM 集成、SSO、地理位置定制和设备软件更新等服务器行为。

Admins 管理员

SafeConsole 管理员页面提供了管理员登录的地理概况。在这里，你可以添加具有特权的管理员并管理他们的访问权限。人员可以选择启用双因素身份验证，并可从管理员账户的个人资料设置菜单中激活（登录后右上角的下拉菜单）。管理员可以在"2-Factor Login"列中验证激活情况。另外，管理员页面还可以强制启用双因素身份验证、启用地理围栏策略以及激活自定义角色。请注意，其中一些设置只能由账户所有者更改。

License Info 许可证信息

许可证页面显示许可证信息、产品手册和下载，并允许管理员刷新现有许可证或安装新的许可证。

Help 帮助

帮助包含一个子菜单，其中包含"部署向导"、"快速连接指南"和"支持"子菜单。

- 部署向导允许你向终端用户发送《快速连接指南》。
- 快速连接指南包含了配置/安装设备和 PortBlocker 或 SafeCrypt 端点的过程。除了这些指南之外，管理员还可以找到大规模部署和遗留帮助。
- 支持页面列出了帮助台、SafeConsole 手册、发行说明和最新的软件更新包的链接。最新的软件更新包。

Connection Token 连接令牌

在"帮助"菜单项下面，可以复制连接令牌的 URL。

将你的第一个设备连接到 SafeConsole

第 1 步：在将驱动器注册到 SafeConsole 之前，必须配置默认策略。如果默认策略尚未配置，请点击网站顶部的红色栏，上面写着"您的设备的默认策略尚未设置！"。这将弹出策略编辑器，你可以设置你的默认策略，并点击保存以确认。这个策略将是所有连接的驱动器的基本和后备策略。

第 2 步：在主菜单中的"帮助"部分，导航到"快速连接指南"。按照文件中概述的步骤进行操作。

确认注册到 SafeConsole

在主菜单中点击"管理->驱动器"或"PortBlocker"，这取决于注册的终端设备。

你的终端设备现在应该是可见的。请注意，每次解锁终端设备时，它们都会获取新的配置和策略。请注意，并不是所有的操作都会显示出来，这取决于终端设备当前的状态。

管理驱动器

驱动器操作

可以在主菜单中的"管理->驱动器"部分对设备进行操作。注意，每次设备软件启动时，设备都会检查要应用的操作。

这些操作如下：

恢复状态

将硬盘设置为中性状态，删除所有待处理的操作。

批准

允许设备成为受管理的设备，并占用一个许可证席位。要启用批准流程，请导航到服务器设置，点击"常规"，找到"注册和密码重置"部分，并勾选"需要管理员批准注册"复选框。

不批准

撤销该设备的注册和许可席位的使用。该设备将成为无人管理的设备。需要在服务器设置下启用批准流程

（见上面的批准部分）。驱动器可以在注册期间或设备处于出厂重置状态时被取消批准。

设置为审计模式

在设备客户端 6.3 中引入的审计模式下，设备无法通过设备密码解锁。相反，每次设备必须通过 SafeConsole 使用忘记密码的过程进行解锁。当在这种模式下解锁时，驱动器被设置为强制只读模式，防止对设备进行任何更改，包括设置一个新的密码。设备上的所有文件都将被索引，日志将被发送到 SafeConsole。要从审计模式中删除一个设备，必须从 SafeConsole 发出一个出厂重置命令。

标记为丢失

在这种状态下，当用户访问设备时，设备将显示一条信息。显示的信息可以在设备状态策略中自定义。注意：这不会阻止对设备的访问。

注册未完成

如果设备已经被添加到 SafeConsole，但需要进一步的行动，这条信息将出现在设备操作下拉菜单中。可以通过在下拉菜单中选择"批准"来注册该驱动器。

重置密码

使工作人员能够在不影响驱动器中存储数据的情况下帮助用户重设密码。忘记的密码永远不会暴露，该方案在密码学上是安全的，不会削弱设备的硬件暴力保护。密码重置只对远程用户进行，其中用户可以通过内部程序进行验证。

只有在提示重置密码操作之前，设备上已经应用并激活了远程密码重置策略，才能进行密码重置。请注意，密码恢复只适用于已经解锁并与 SafeConsole 连接的设备。

以下是执行密码重置的步骤：

1. 打开设备软件，获得八个字符的客户端请求代码（密码 ID），该代码可以在设备软件主页上的忘记密码链接下找到。(注意：此步骤可以在 SafeConsole 的"服务器设置>常规"部分禁用）
2. 在 SafeConsole 中，搜索以找到驱动器或用户下的设备。验证设备 ID 或序列号，该信息位于客户端的"关于"或"设备信息"下。
3. 在 SafeConsole 中为该设备选择"重置密码"操作。
4. 如果启用，在 SafeConsole 的提示中输入客户请求代码（密码 ID）。
5. 将显示 24 个字符的服务器响应代码，你可以点击把它发送到注册设备用户的电子邮件地址。你也可以把这个字符串读给设备用户。请确保准确获取字符串，因为错误的代码会破坏所有存储的数据。我们建议采用音标字母表来进行传输。
6. 设备用户在设备软件中输入响应代码，现在将提示创建一个新的设备密码。

禁用

对于运行 6.x 客户端的设备：

禁用解锁设备的功能。仍然可以执行密码重置，前提是在提示禁用操作之前，已经在设备上应用和激活了远程密码重置策略。为了再次访问该设备，需要将其状态改为"In Use"。注意：执行密码重置将使设备恢复为"In Use"状态。

对于运行 4.8.x 客户端的设备：

禁用解锁设备的功能。禁用设备将要求用户执行密码重置或出厂重置，以便再次使用。为了执行密码重置，在提示禁用操作之前，必须已经在设备上应用并激活了远程密码重置策略。注意：执行密码重置将使设备恢复为"In Use"状态。

拒绝访问

只适用于运行 4.8.x 客户端的设备

拒绝对设备的访问。该设备将无法解锁，直到管理员恢复对该设备的访问。然而，它仍然会收到从 SafeConsole 发送的操作命令。为了再次访问设备，需要将状态更改为"In Use"。注意：执行密码重置将使设备恢复为"In Use"状态。

出厂重置

出厂重置操作，有时也被称为远程清除，在下一次连接时，会从设备上不可恢复地删除加密密钥和所有存储的数据。该设备可以被重新使用并重新连接。

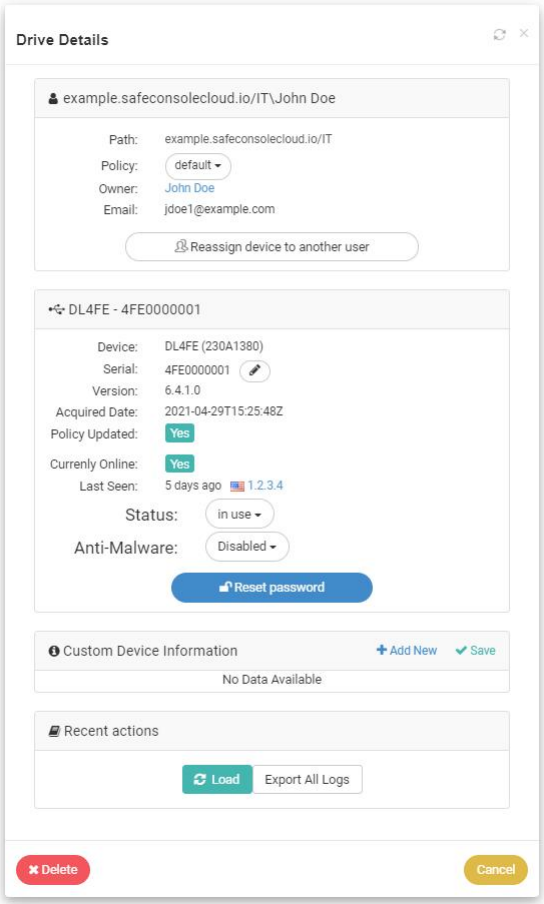
引爆

引爆操作只适用于 DataLocker H300、DataLocker H350 和 IronKey S1000 设备。这个操作类似于"出厂重置"，但如果没有恢复驱动器使用的过程，将使驱动器无法使用。在选择这个操作时，请谨慎行事。

查看和编辑设备和用户数据

驱动器数据

在主菜单选项 "驱动器"中的"序列"栏，你可以点击受影响的设备或弹出的窗口按钮，打开"驱动器详细信息"窗口，查看或编辑服务器上设备的数据。



- OU 路径
- 分配的策略
- 所有者信息：包括将设备重新分配给另一个用户（这不会改变设备的密码，还应进行密码重置）
- 设备型号
- 序列号
- 软件版本
- 获取日期：设备注册到 SafeConsole 服务器的日期。
- 策略更新：设备是否存在当前策略（是或否）。
- 在线：是或否
- 最后出现：自最后一次连接以来的小时/天数，以及最后使用该设备的工作站的 IP 地址
- 存储信息：已使用的空间和总大小（需要 6.1 或更高版本的软件来填充）。
- 当前状态

- 反恶意软件状态
- 重置密码
- 编辑自定义数据：更多信息见自定义信息
- 最近的操作：加载或导出所选设备的审计日志条目
- 删除设备：将设备从数据库中删除，并将设备保留在它的当前状态

状态

这将允许你改变所选设备的状态。选项将包括所有可用的操作，如恢复、标记为丢失、拒绝访问、出厂重置等。

反恶意软件状态

这将允许你改变所选设备的反恶意软件状态。选项将包括在"驱动器"页面上列出的相同操作，如通过策略配置、始终启用、始终禁用等。

重置密码

这使您能够在不影响设备的存储数据的情况下重置你的密码。

注意：只有在提示重置密码操作之前，已经在设备上应用和激活了远程密码重置策略，才能执行密码重置。

重新分配

这将允许你指定一个新的用户作为设备所有者。它可以将设备分配给任何其他注册用户。

编辑自定义数据

允许管理员编辑在设备设置期间收集的数据（如果在策略中的自定义信息下配置）。

最近的操作

允许管理员加载由所选设备执行的所有操作的列表。这些日志也可以被导出为 CSV 或 XML 文件。

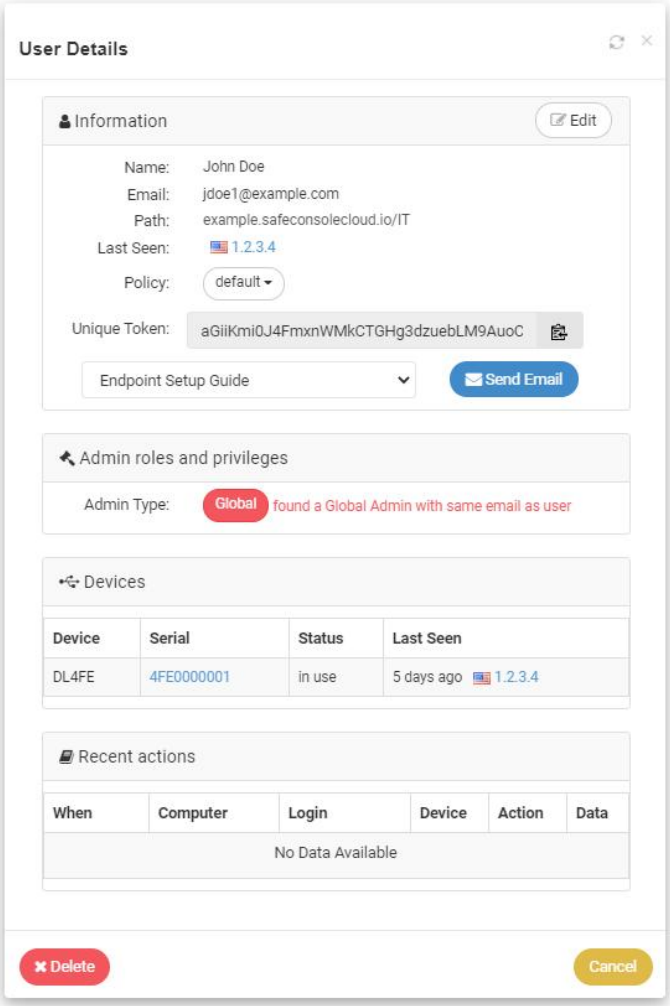
删除-设备

这将从服务器上删除设备，除非在服务器设置中启用了可选的回收站功能。如果启用，删除一个设备会把它移到回收站中。回收站中的设备不占用许可席位。回收站中的设备既可以被恢复，也可以被永久删除。

当设备被永久删除时，应该小心，因为这个操作是不可逆的，有可能导致设备不再处于有效状态。建议只永久删除处于出厂重置状态的设备。

用户数据

在主菜单选项"用户"中，在"用户"一栏，点击受影响的用户，打开"用户详细信息"窗口，查看或编辑服务器上的用户数据。你也可以在这里删除该用户。



- 用户信息：包括一个编辑按钮来编辑用户信息
- OU 路径
- 最后出现：自最后一次连接以来的小时/天数，以及该设备最后使用的工作站的 IP 地址
- 分配的策略
- 唯一用户令牌

- 发送电子邮件
- 管理员角色和权限：如果用户的电子邮件与管理员的电子邮件相对应，则显示管理员权限的级别
- 设备：设备列表，包括设备类型、序列号、状态和最后在线时间信息
- 最近的操作：允许管理员加载与所选用户相对应的审计日志列表
- 删除用户：从数据库中删除该用户

编辑用户信息

编辑按钮允许你更改用户账户上的信息，如他们的姓名、电子邮件地址或 OU 路径。

发送电子邮件

这个选项允许你向选定的用户发送他们的唯一用户令牌，以便注册设备。电子邮件模板可以在服务器设置下的自定义电子邮件模板部分进行编辑。

删除-用户

这将从服务器上删除用户。已分配设备的用户不能被删除，除非将这些设备重新分配给其他用户或被删除。

导入包含用户数据的 CSV 文件

如果你只有一个策略，或者不会预先配置和重新分配设备给终端用户，首选的部署选项是使用终端用户的设备凭证让数据库自动填充。这种设备所有权操作可以在服务器设置中的注册和密码重置部分进行配置。有了这个选项，数据库将在用户连接设备时用目录结构填充 SafeConsole 中的用户。

然而，也可以导入一个标准化的 CSV 文件，其中包含您的用户和组。然后，可以使用导入的结构在用户连接到服务器之前应用策略。

- CSV 文件应该包含以下字段：区分的名称和电子邮件地址
- 建议每次导入的最大条目：1000 个

使用 Windows PowerShell 命令创建一个 csv 文件：

Get-ADUser -Filter * -Properties DisplayName,EmailAddress |export-csv ad_users.csv

关于 Get-ADUser 命令的其他帮助，请访问微软的知识库

从 Active Directory 中生成 CSV 文件后，你可以通过点击"管理"下的"用户"选项卡中的"导入 CSV"来导入该文件。这将根据用户在 Active Directory 中所属的组织单元将用户放在路径中，从而填充 SafeConsole 服务器。

有关此过程的其它帮助，请参考这篇支持文章：将 Active Directory 用户导出 CSV 文件

在完成导入之前，你需要提供 CSV 文件的字符编码（US-ASCII，UTF-8 或 UTF-16）。

你可以选择向用户发送一封电子邮件，其中包含"终端设置指南"。要实现这一点，请勾选"向所有用户发送电子邮件"的复选框。选中该复选框后，你可以从三种版本的指南中选择。管理员可以通过在自定义电子邮件模板设置中找到模板来编辑发送的电子邮件。

策略-配置密码策略和功能

Policies 部分可通过位于"manage->policies"下的主菜单访问。

每次设备解锁时，都会检查并应用策略，以实现与 SafeConsole 的连接。

有蓝色的内联帮助文本和更多信息图标，将解释每个策略部分的每个可用选项。

策略部分导航概述

- 默认策略可以通过点击顶部栏中的"修改默认策略"按钮进行修改。默认策略是所有其他策略所基于的后备策略。你必须点击，配置并保存默认策略，才能完成服务器的设置。新的设备和终端注册将使用默认策略，包括在地理位置和受信任网络部分发现的访问限制，除非在服务器上启用了唯一令牌。
- 你可以使用路径栏中的扳手菜单来编辑路径。管理员可以使用此功能执行以下操作：
  - 添加新用户：在相应的路径上添加一个用户。
  - 添加新组：创建一个新的路径，作为相应路径的子节点。
  - 导入 CSV：将多个用户添加到相应的路径中。CSV 需要一个特定的格式。更多信息请参阅：从 CSV 中添加用户。
  - 编辑路径：更改相应的路径。
  - 删除路径：如果路径中没有用户，则删除相应的路径。
- 点击顶部的"添加新路径"，可以创建一个新的路径。
- 策略表中显示的列，可以从顶栏的列下拉菜单中自定义。

策略编辑器

- 当点击"修改默认策略"按钮或从策略栏的下拉菜单中选择"创建"或"修改"时，策略编辑器就会弹出。

策略编辑器显示所有的策略配置，每个策略在本手册中都有详细介绍。在策略编辑器的每个部分，你可以验证更改将应用于哪个策略版本号。默认情况下，使用的是基础和回退策略。

点击策略栏内的下拉菜单，然后点击"创建新的自定义策略"，即可创建一个自定义策略。然后将创建一个

名称为"custom #incrementing-number"的自定义策略，例如，custom #56。自定义策略可以应用于有组（子路径）的路径。在这种情况下，组将从主路径继承其配置。这些被标记为"inherit #custom-incrementing-number"，例如，inherit #56。一个组的策略可以被修改，以打破这种继承，并使用一个单独的自定义策略。请注意，通过删除组的自定义策略可以恢复为继承状态。

策略过滤

并非所有终端都支持所有策略。要查看每个终端适用的策略，请使用策略编辑器顶部的按钮来过滤适用的策略（如 v6.x、K300、DL3/DL3FE 等）。当应用过滤器时，对任何策略部分的更改将应用于所有适用的终端。例如，不可能为 Windows 设置一个策略，为 macOS 设置另一个策略。此外，如果一个策略适用于多个终端，它将在每个部分被更改，如密码策略。

注意：一些策略要求你的设备更新到某个客户端版本（或更高版本）。

将策略应用于路径

在路径列中，你可以看到域路径，在策略列中，你可以为路径修改或创建一个新的策略。当选择"创建或修改"时，策略编辑器将弹出。

要确认该策略适用于哪些用户和驱动器，请点击相应列的蓝色链接。

策略-用户默认值

在策略编辑器弹出窗口中可用

用户默认值策略允许你管理设备的软件行为。

以下配置是可用的：

- 禁止用户重置设备
    - 禁止用户重置他们的设备。重置后，设备可以变为非托管状态，或由不同的 SafeConsole 服务器管理。这个选项允许你防止用户重置他们的设备，从而删除你的 SafeConsole 控制。管理员仍然可以执行出厂重置操作。请注意，如果服务器在设备注册时被卸载，这些设备就不能被重置，也不能被任何其他服务器所管理。如果使用 On-Prem，请格外注意保存你的服务器证书的副本、服务器证书密码，并确保在旧服务器宕机时主机名可以分配给新的服务器。
- 禁止用户格式化设备存储
    - 例如，设备客户端允许用户将设备格式化为不同的文件系统。这个过程将删除用户的数据，如果用户未经培训，可能会导致数据丢失。这个选项允许管理员防止这种情况的发生。
    - 需要设备客户端 6.3.2 以上版本
- 禁止用户对设备进行消毒
    - 设备消毒会擦除数据，删除加密密钥并重新发放加密密钥。这个过程类似于出厂重置功能，但允

许设备保留 SafeConsole 管理。这个过程将删除用户的数据，如果用户没有经过培训，可能会导致数据丢失。这个选项允许管理员防止这种情况的发生。

  - 需要设备客户端 v6.3.2+。

- 解锁屏幕信息
  - 在解锁过程中向设备用户显示一条信息。这个信息可用于提供设备的所有权信息。
  - 可以将该信息设置为允许用户在设备解锁后进行修改。
  - 需要设备客户端 6.3 以上版本
- 启用控制面板应用程序列表
  - 默认情况下，用户可以在设备控制面板上创建文件或程序的快捷方式。启用后，用户可以在设备解锁后右键单击并选择"添加应用程序"。管理员可以取消勾选该选项来阻止这一功能。
  - 需要设备客户端 6.2 以上版本

策略设备用户交互

用户将看到一条消息，说明策略配置已更新，并提示用户锁定、拔掉插头和解锁以完成策略更新。然而，任何配置都将被强制在设备上进行。

策略-反恶意软件

在策略编辑器的弹出窗口中可用

通过板载反恶意软件保护，可以自动并始终保护您的设备免受恶意软件的侵害。当设备解锁时，如果有可用的互联网连接，恶意软件签名定义数据会自动更新。该功能由英特尔安全公司的 McAfee 技术提供。

板载反恶意软件保护仅适用于 Windows 4.8.30 及以上版本和 macOS 6.1.2 版本的设备客户端。每台设备都需要购买反恶意软件许可证。请注意，该许可与设备许可是分开的。

以下配置是可用的：

- 启用反恶意软件保护
  - 为分配到此策略的设备启用板载反恶意软件保护。
  - 威胁检测、修复和签名更新将在用户审计日志中可见。
- 限制设备登录，直到反恶意软件更新完成。
  - 在允许设备解锁之前加载完整的反恶意软件定义。
  - 将增加解锁设备所需的时间。

- 需要设备客户端 v 6.3 以上

- 隔离受感染的文件
  - 默认情况下，反恶意软件将删除检测到的受感染文件。隔离文件存储在驱动器的安全分区上，用户可以恢复或删除这些文件。不能被隔离的项目将被删除。
  - 要求设备客户端 6.3.1 以上

- 反恶意软件定义的自定义 URL
  - 默认情况下，使用 McAfee 面向外部的定义存储库。这允许管理员选择自定义位置。
  - 需要设备客户端 6.3+版本

反恶意软件可以从"修改策略"页面、"用户详情"窗口或"驱动器"页面中进行切换。

在支持的设备上，McAfee 反恶意软件客户端软件直接从 McAfee 的 update.nai.com 服务器下载病毒定义文件更新。

如果你使用 SafeConsole 管理支持的设备，则可以配置设备从你指定的位置，如本地托管的服务器，下载病毒更新（.DAT）文件，以减少互联网带宽使用。

策略设备用户交互

用户不会被提醒该策略已激活。设备软件将在下次解锁并有网络连接时自动从 McAfee 服务器下载最新配置。在初始下载过程中，设备可能会出现异常延迟，直到签名数据库完全下载完毕（大约 200MB）。一旦数据库被下载，设备将在每次解锁时在后台启动扫描程序。该扫描程序连续运行，并扫描会话期间添加的任何文件。受感染的文件会被删除，并提示用户已经发生了这种情况。

一旦设备被解锁，用户可以在主菜单中的反恶意软件按钮下与反恶意软件进行交互。点击该按钮后，将显示反恶意软件界面。在反恶意软件屏幕上，用户可以验证保护的状态和上次扫描的时间。用户还可以手动启动额外的扫描。此外，用户可以验证引擎和恶意软件数据库的版本以及上次更新的时间。用户还可以手动启动恶意软件数据库的更新。正常操作下，这没有必要触发，因为更新会自动进行。

如果启用了隔离功能，用户将在主菜单中看到另一个标有"隔离"的按钮。点击这个按钮时，将显示"隔离"界面。如果有任何检测到的文件，它们将在此屏幕上列出。选择后，用户将看到其他信息，包括威胁名称和威胁类型。此外，用户可以选择恢复该文件或永久删除文件。

策略-设备状态

在策略编辑器的弹出窗口中可用

设备状态策略可以实现驱动器的自动库存管理。

以下配置是可用的：

- 给用户的丢失驱动器信息：文本字段

- 管理员可以自定义设备进入丢失状态时向用户显示的信息。
- 当设备被标记为丢失时，将显示此信息。这个文本可以是："请归还至指定地址"或包含一个通知或免责声明。

- 要求设备连接到 SafeConsole 服务器的复选框
  - 选择这个复选框，可以要求设备定期连接到 SafeConsole 并定义条件。最近的连接会显示在"驱动器"部分的"Last Seen"列。你可以定义设备在不连接到 SafeConsole 的情况下保持在用状态的最大天数和小时数（需要设备客户端 v6.3.2+）。你还可以定义在指定窗口外连接的任何设备上强制执行的状态（丢失、拒绝访问或禁用）。
  - 这些是可用的配置选项：
    - ✓ 定期（下拉列表）
      - 配置没有连接的最大天数和小时数。请注意，设备客户端 v6.3.2+需要使用定义的小时数。否则，设备将只利用天数。
      - 同时配置选择器在达到最大天数后，将状态设置为：
      - 丢失(只显示丢失信息)
      - 拒绝访问（阻止设备访问），可以通过恢复状态操作取消
      - 禁用（对于 4.8.x 设备需要重置密码），可以通过 SafeConsole 重置密码来取消。如果当设备收到设备状态策略时，设备上的远程密码重置策略是不活跃的，那么它将需要一个出厂重置操作。
      - 没有连接的最大登录次数，需要 v6.2+。配置在阻止登录和设备需要联机之前，设备可以脱机解锁的次数。
    - ✓ 始终（下拉列表），需要设备 v4.8.25 以上版本。您可以使用 ZoneBuilder 的限制设备访问功能，更好的控制离线使用。

策略设备用户交互

用户不能与策略配置互动，也不会收到策略已激活的提示。任何配置的设备状态将在达到定义的最大允许天数、小时数或登录次数时自动强制执行。请注意，当用户接近配置的最大允许天数、小时数或登录数时，他们将收到提醒。如果你的策略配置为始终需要连接，则当用户无法连接到 SafeConsole 时将收到警报。

策略-非活动锁定

在策略编辑器的弹出窗口中可用

启用后，该策略会激活一个具有可配置的不活动时间限制的自动锁定机制。这个选项应该被启用，因为设备解锁后经常被遗忘在主机中。如果没有"不活动锁"，你就有数据泄露的风险。

以下配置是可用的：

- 用户配置：激活后，允许用户在解锁后的设备软件菜单中配置不活动时间限制。
    - ✓ 由策略强制执行：通过 SafeConsole 设置非活动锁定。
    - ■ 允许设备使用不活动锁：勾选此设置复选框来管理非活动锁定设置。这将覆盖本地用户设备设置。一旦激活，你将定义设备因不活动而被锁定前的分钟数。
        - ✓ 超时（分钟）：以数字方式输入(限制 2-261)

策略设备用户交互

如果由策略强制实施，用户不会收到有关策略已激活的警报，并且他们将无法与策略配置交互。如果该策略设置为"用户可配置"，则用户可以在设备解锁后显示的主菜单中的设置下调整超时时间。

策略-授权的自动运行

可在策略编辑器的弹出窗口中使用

该设置仅适用于设备客户端 6.2-6.3 版本，对于设备客户端 6.3.1 及以上版本已被删除。

以下配置是可用的：

- ✓ 使用此设置，在所有设备上启用授权自动运行，指定在用户认证后在所有设备上运行的命令。在提供的文本字段中输入要运行的具体命令。授权自动运行允许 SafeConsole 管理的设备在认证后运行便携式软件或其他安全工具。
- ■ "要运行的命令"文本框中，键入要运行的命令。
- ■ 以下令牌对你来说是可用的，可以在命令中使用。
    - ✓ {store-path}：设备加密的存储分区卷
    - ✓ {serial}：设备的设备 ID
    - ✓ {login-path}：设备的 CD-ROM 分区卷
    - ✓ {user-name}：设备用户的注册用户名
- ■ 输入一个网站 http://www.example.com，以便在设备解锁时在默认浏览器中启动。

同时运行多个命令的例子

可以通过在*.cmd 批处理文件中输入多个命令来指定要运行的命令。可以将令牌发送到脚本中，并设置为本地变量。

要运行的命令的例子：

{store-path}/Applications/cmd/scr.cmd{ serial} {store-path}

这些是*.cmd 文件的示例行。在本例中，我们运行带有参数的 Allway Sync'n'Go 应用程序，Allway 应用程序使用本地设置的变量来定位本地和目标目录。

@ECHO OFF

SET SCRID=%1 && SET SCRVOLUME=%2

第一行使进程静默。第二行从授权自动运行命令中获取设备的序列号和存储路径。

START /D ^"%2Applications\Allway^" AllwaySync'n'Go.exe -m

这个示例行专门启动 Allway 便携式同步应用程序。参数-m 是 Allway 特有的，表示应用程序以最小化的方式启动。

START /D ^"%2Applications\Example^" Example.exe"

最后一行是为了证明我们也可以从这个批处理文件中运行其他的应用程序。

策略设备用户交互

用户不能与策略配置交互，也不会收到策略已激活的提醒。用户会看到由命令提示运行的任何软件或文件。

策略-密码策略

在策略编辑器的弹出窗口中可用

该策略允许您配置详细的密码策略。

以下配置是可用的：

- 强制执行强密码（符合 FIPS 140-2 标准）
  - 对密码设置以下限制
    - ✓ 长度必须至少为 8 个字符。
    - ✓ 必须包含以下至少 3 个类别中的字符。
      - ASCII 数字
      - 小写 ASCII 字母
      - 大写 ASCII 字母
      - 非字母数字的 ASCII 字符
      - 非 ASCII 字符

- ✓ 如果密码的第一个字符是一个大写的 ASCII 字母，则不计为大写的 ASCII 字母，不适用于限制 2。
- ✓ 如果密码的最后一个字符是一个 ASCII 数字，则不计为 ASCII 数字，不适用于限制 2。

使用其他设置来定义最小密码长度和所需的数字、小写字母、大写字母和特殊字符。请注意：对于 FIPS 认证的硬件，建议密码长度至少为 8 个字符。对于 v6.2 以上版本，最小长度不能低于 8 个字符。

* 最小密码长度

* 要求数字字符（1,2,3...）。- 复选框

* 要求小写字符(a, b, c...)。- 复选框

* 要求特殊字符(#, !, ?...)。- 复选框

* 设备的密码在#次登录后过期 - 以数字输入。

* 设备的密码在#天后过期 - 以数字输入。

请注意，NIST 指南预览建议不要强制更改密码，因为这可能导致用户选择"更简单"的密码。

- 默认情况下最大失败的解锁次数，设备在发生暴力破解操作之前，会允许 10 次登录尝试。本节允许你配置这个最大的失败尝试次数（最小为 2）。
  - 保存远程密码重置的最后尝试
    - ✓ 如果选择"是"，当设备达到允许的解锁尝试的最大限制时，将进入不使用的状态。设备可以使用密码恢复流程来恢复。
    - ✓ 如果选择"否"，设备将执行选定的暴力破解操作。
  - 暴力破解操作
    - ✓ 允许你选择当达到最大限度时，设备是否会出厂重置或引爆设备。如果设备不支持引爆功能，它将恢复到出厂设置。

策略用户交互

在首次设置设备或下次解锁设备时，将检查密码是否符合现行策略。一旦连接到服务器，该策略将显示在欢迎屏幕上，或者如果发现当前密码不符合现行策略，将强制显示在更改密码屏幕上。用户必须遵守密码策略才能继续操作。Bruteforce 将以类似的方式显示。一旦达到最大的解锁尝试限制，设备将执行选定的操作。如果配置了密码重置，用户将在密码重置完成之前无法继续操作。如果发生恢复出厂设置或引爆操作，用户将在设备上执行操作后看到一个结果弹窗。

策略-远程密码重置

在策略编辑器的弹出窗口中可用

该策略允许 SafeConsole 工作人员协助设备用户从忘记的密码中恢复，而不会丢失任何存储信息。该技术以密码为基础，不会削弱设备的安全性，因为所有重置密码的尝试都是根据设备安全控制程序验证的。

一旦启用，设备必须在连接到服务器的情况下解锁一次，才能应用该配置。设置完成后，可以随时进行远程密码重置。远程密码重设不需要互联网连接。

不可能在事后激活策略来恢复现在已经忘记的设备密码。因此，建议始终启用该策略。

以下配置是可用的：

- 启用密码重置
    - 选择这个复选框，使用户能够请求远程密码重置。你还可以定义应该发送密码重置请求的电子邮件地址（通常是 support 邮箱），用户可以拨打的电话号码（可选），以及从 SafeConsole 发送给用户的密码重置电子邮件的主题行。
    - 支持电子邮件地址：在文本框输入一个有效的邮箱地址。该电子邮件显示在设备软件中，使用户能够联系您的支持人员。(最多 32 个字符)
    - 支持电话号码：以数字形式输入。这个号码会显示在设备软件中，以便用户与您的支持人员联系。(最多 15 个字符)
    - 密码重置邮件主题：文本框用于设置密码重置邮件的主题。由设备用户发送到上面定义的支持电子邮件地址。

策略设备用户交互

用户的设备在下次使用 SafeConsole 连接并解锁设备时，会自动加入远程密码重置程序。用户不会被提示，但在设备登录屏幕上会出现"忘记密码"的选项。点击此按钮将显示执行远程密码重置所需的配置的联系信息和密码 ID。在此屏幕上，用户将输入 SafeConsole 工作人员提供的响应代码，以启动密码重置并选择一个新的合规密码。

如果你没有在 SafeConsole 中为用户注册电子邮件地址，设备软件将提示用户输入并确认他们的电子邮件地址。该消息声明，该地址可用于未来的密码重置，并且只与私有 SafeConsole 服务器的工作人员共享。

请注意，如果密码重置是在离线情况下进行的，用户将需要解锁连接到 SafeConsole 的设备，并备份适当的密码，以便将来进行密码重置。

策略-写入保护

在策略编辑器的弹出窗口中可用

启用写保护是一个强大的反恶意软件措施，因为当它被激活时，没有文件可以被复制到设备上。当不需要复制文件到设备上时，建议在未知机器上解锁设备时使用这个选项。例如，在演示过程中。

以下配置是可用的：

- 在设备上启用写保护
  - 选择这个复选框，对所有设备实施写保护。这将允许用户读取注册设备上的数据，但不允许他们更新或删除数据。
  - 写保护模式选择器。可用的模式有：用户可配置（允许终端用户选择将设备解锁为只读），在可信区域外激活，或始终强制执行只读模式。
  - 可信任区 Trusted Zone
    - ✓ 通过可信网络策略进行配置
    - ✓ 通过可信证书策略配置。注意：只有 CA 签署的证书才对该策略有效。

例如，这个策略可用于一组用户，你想允许他们在网络外做演示，但不允许他们把文件带回网络上的设备。

策略设备用户交互

用户不会收到策略已激活的提醒。

如果策略被设置为"用户可配置"，则在主屏幕的"输入密码"下会出现一个复选框，并显示"只读模式下解锁"的字样。如果勾选此选项，设备将在只读模式下解锁为写保护。系统将提示[device_brand]，已被只读解锁。

如果配置了"在可信网络外激活"，则设备将被强制进入该模式，并且用户将收到通知。因为您在可信网络之外，因此[device_brand]已在只读模式下解锁。

策略-文件限制

在策略编辑器的弹出窗口中可用

你可以允许或限制适用于设备的安全存储分区的文件扩展列表。这个选项可用于加强反恶意软件保护，因为可执行文件格式可以在可移动媒体上受到限制。该功能只对文件扩展名进行过滤，但这意味着这些文件将不能在主机上运行，因此不需要分析文件头。

注意：文件限制将允许设备客户端直接在驱动器上放置文件，包括反恶意软件和发布者所需的文件（如果适用）。

以下配置是可用的：

- 启用设备上的文件限制复选框
  - 选择此复选框可以限制用户可以保存到其设备上的文件类型。你还可以定义哪些文件扩展名受策略影响（例如.exe、.dll 等），以及限制模式，允许你限制或允许。如果你选择"限制"，用户将不能保存你指定的文件类型到他们的设备上。如果你选择"允许"，用户将只能保存你指定的文件类型到他们的设备上。
  - 文件类型扩展-文本输入。在这里输入你想改变权限的文件类型，文件扩展名用逗号隔开，如：

exe，dll，com...

- 限制模式
  - ✓ 限制这些文件（黑名单）：设备软件将立即删除任何与文件类型扩展名中列出的文件扩展名相符的文件。
  - ✓ 只允许这些文件（白名单）：设备软件将立即删除任何不符合文件类型扩展名中所列文件扩展名的文件。

文件类型扩展名输入示例

限制以下可执行文件格式是常见的做法：exe, dll, com, bat, js, jse, msi, msp, ocx, reg, sct, scr, sys, vb, vbe, vbs, wsc, wsf

策略设备用户交互

用户不会收到策略已激活的警报。如果一个文件被阻止存储在安全存储分区上，用户会被通知有些文件被阻止以保护你的计算机：[文件路径列表]。该文件将从设备的安全存储中删除。注意，你可能需要刷新文件资源管理器以确认删除已完成。

策略-设备审计

在策略编辑器的弹出窗口中可用

默认情况下，对所有设备操作（如解锁）和文件审计（跟踪文件的创建、删除和移动（重命名）是启用的。如果需要，你可以禁用此审计。也可以限制你的文件审计，只跟踪某些文件扩展名。

注意，当设备正在读取或复制文件时，文件审计将不可用。它们将在设备完成后更新。

清晰的审计日志通常是符合法规遵从要求的，因此建议保持启用这些策略。

日志会在下次设备解锁时同步（通过 SafeConsole 连接）。日志从加密的本地缓冲区加密上传，该缓冲区位于设备的隐藏存储区分区中。记录的时间是上载到 SafeConsole 服务器的时间。

日志可以在 SafeConsole 的主菜单选项"审计日志 > 用户审计日志"下搜索到。

对于内部部署安装，审计日志将一直保存，直到从日志文件夹中删除。对于云部署，它们至少保存两年，然后在必要时被清除。

以下配置是可用的：

- 在所有设备上启用审计复选框
  - 选择此复选框以捕获所有设备活动的审计日志（连接、失败的登录尝试、密码重设等）。
- 启用详细的文件审计复选框

- 选择此复选框来捕获保存到设备或从设备移除的所有文件的审计日志。所有文件类型都会被记录。
  - ✓ 文件类型扩展-文本输入。输入你想审计的文件类型的扩展名，用逗号隔开，例如 pdf, docx, ppt。

策略设备用户交互

用户不会收到策略已激活的提醒，也不会影响策略。

策略-自定义信息

在策略编辑器的弹出窗口中可用

这个策略允许你在注册时从设备用户那里收集最多三个文本字符串（令牌）的信息。

每个令牌都有：

- 令牌名称（可用于脚本的对象名称，例如：room_number），在其他策略中使用时的标识符。令牌名称只能包含字母、数字、连字符、下划线和句号。它必须以字母或下划线开头。例如：room_number、full_name
- 令牌描述（便于显示的名称，例如：房间号），它将在设备软件中显示，以便设备用户了解在该字段应该输入什么。例如。办公室房间号，全名

以下配置是可用的：

- 在所有设备上启用设备用户信息复选框
  - 收集的数据将显示在 SafeConsole 的驱动器部分，并可用于授权自动运行策略的脚本。
  - 每个令牌名称应该提供令牌描述。
  - 令牌 1：标签，要收集的第一项信息，提供两个文本输入框。
    - ✓ 令牌名称，文本输入
    - ✓ 令牌描述，文本输入
  - 令牌 2：标签，要收集的第二项信息，提供两个文本输入框。
    - ✓ 令牌名称，文本输入
    - ✓ 令牌描述，文本输入
  - 令牌 3：标签，要收集的第三项信息，提供两个文本输入框。
    - ✓ 令牌名称，文本输入
    - ✓ 令牌描述，文本输入

自定义信息收集的元数据将作为单独的列显示在主菜单的"管理 > 驱动器"部分的表格中。请确保在右上角的选项菜单中启用列的显示。点击菜单外的区域以关闭它。数据将根据你的选择进行更新。

一旦数据被收集，工作人员可以使用"编辑自定义数据"选项在服务器上更新。

自定义信息可以在"修改策略"页面或"驱动器详情"窗口中找到。

策略设备用户交互

当策略被激活时，用户将被提示输入所需的信息。这将在他们下次与 SafeConsole 连接解锁时。将显示一个独立的屏幕，以"设备设置"作为标题，显示配置的文本输入框，以及一个完成收集的继续按钮。此外，用户可以通过点击"工具>关于我"，在设备软件中重新访问这些字段。

策略-ZoneBuilder

在策略编辑器的弹出窗口中可用

当启用时，ZoneBuilder 会在策略（强制执行或用户可配置）调用时，在计算机上安装一个本地证书，并解锁该证书。计算机可以在受信任的网络策略中定义。该证书将安装在用户账户的"MY STORE"证书存储中，任何人都不能导出。有了这个证书，设备将被视为在受信任区域。通过这个证书和受信任网络策略，你可以配置受信任区域。ZoneBuilder 利用这个证书来启用密码功能，使解决方案的安全性更严格或更方便。请注意，随着采用率的提高和对策略的遵守，增加用户的便利性也可能意味着更好的安全态势。

一旦启用，该功能无法完全停用，因为这将需要重新设置设备以重新生成证书。警告：如果 SafeConsole 服务器和 ZoneBuilder 证书不可用，配置了 ZoneBuilder 策略的设备可能会无法操作。请采取措施，以确保这不会发生，以避免无法访问设备。

ZoneBuilder 可以通过限制设备访问执行更高的安全性：

1. 只允许在已安装的可信证书或可信网络所定义的配置的可信区域内解锁。

2. 只允许目前在可信网络内的设备解锁。这个选项意味着设备在网络外根本无法解锁，这是一种强大的方式，允许在安全网络上或在安全网络之间进行数据传输。

为了方便，ZoneBuilder 可以启用自动设备解锁：

1. 允许自动解锁受信任机器上的设备。这种设置使终端用户的工作日更加方便，并提高了设备的采用率。由于用户必须对他们的用户账户进行认证，安全性仍然很高。在其他机器上解锁时，用户仍将使用他们的设备密码。

2. 作为自助式密码重置服务使用。如果用户忘记了他们的密码，他们可以把他们的设备连接到受信任的用户账户，然后能够重置密码。不会丢失数据。

3. 用于在团队成员的机器上解锁，而无需分享设备密码。通过允许用户信任其团队成员的用户账户，用户只需要输入一次设备密码就可以启用信任。他们可以自行完成此操作，不需要暴露密码。以后可以从设备控制面板上撤销信任。这提高了生产力，在 WiFi 稀缺或网络被严格封锁的情况下，是快速共享数据的理想选择。

注意，用证书解锁设备会带来额外的安全风险。应谨慎地保护证书的私钥，如不允许私钥导出。

以下配置是可用的：

- 启用 ZoneBuilder 复选框
  - ZoneBuilder 可以用来自动解锁设备（主要是为了方便使用），也可以基于客户端证书限制可以解锁设备的计算机用户账户（限制设备的使用）。所有被允许的受信任计算机用户将成为受信证书的一部分。
  - 限制受信任的计算机使用 CA 签署的客户端证书
    - ✓ 否-允许设备软件生成证书。选择'No'可以让用户轻松将设备与他们选择的计算机进行连接。
    - ✓ [A selected CA cert]这将要求主机上有配置的 CA 的客户端证书，才能使用 ZoneBuilder。
    - ✓ 点击"证书"（扳手图标），显示当前可用的证书（可以通过点击名称旁边的垃圾桶图标删除）。还有一个"添加新证书"的按钮。该按钮将弹出一个"添加新证书"的窗口，你可以在文件浏览器中选择证书，并在文本输入框中输入密码（只对 PKCS12 文件有要求）。该证书必须是 PKCS12 文件或 X509 证书。X509 证书必须是 DER 或 Base64 编码的。
    - ✓ 还有一个可用的链接-如何生成证书，以协助用 OpenSSL 创建新证书。
- 限制设备访问
  - 只允许在可信网络内链接的计算机上使用设备。在第一次成功解锁后，设备将被链接到用户的计算机。然后，该设备可以在可信网络之外或脱机时使用，但只能在链接的计算机上使用。
    - ✓ 要求受信任的计算机用户拥有 ZoneBilder 证书。如果计算机上没有安装匹配的 CA 签名证书，驱动器访问将被拒绝。这个策略需要客户端 6.3.1 版本来执行。勾选后，即使连接到没有安装正确证书的 SafeConsole，设备也将无法被访问。
    - ✓ 要求受信任的计算机用户连接到 SafeConsole。在离线时和在受信任网络之外时，驱动器访问将被拒绝。
- 自动设备解锁
  - 在受信任的计算机用户上自动解锁设备。在设备与用户的计算机连接并建立信任后，允许在用户的计算机上自动解锁设备（无需密码）。
    - ✓ 要求受信任的计算机用户连接到 SafeConsole。在离线状态下或离开受信任网络时，设备将不会自动解锁。
- 受信任网络
  - 通过受信任网络策略进行配置

策略设备用户交互

根据设置不同，会发生不同的交互。

- 将受信任的计算机限制为 CA 签名的客户端证书设置为否，并激活在受信任的计算机用户上自动解锁设备。
    - 用户不会收到激活策略的提示，但是当单击主菜单窗口下的设置按钮时，将显示 ZoneBuilder 部分。ZoneBuilder 设置标题后面是一个"信任此帐户"复选框。用户会收到以下文本提示：当您在受信任的帐户上使用[设备名称]时，您无需输入密码即可解锁。还可以单击"显示受信任的帐户"按钮，显示受信任帐户的概览，在此视图中，用户可以通过单击每个条目上的减号用户图标来确认和撤销信任。
- 将受信任的计算机限制为 CA 签名的客户端证书设置为[选定的 CA 证书]，并激活在受信任的计算机用户上自动解锁设备。
    - 系统将提示用户"信任该用户帐户"以启用自动解锁功能。建立信任后，设备将在安装了相同证书的任何计算机上解锁。ZoneBuilder 设置可在主菜单的设置下找到。

策略-发布者

在策略编辑器弹窗中可用。

此设置仅适用于设备客户端版本 6.2 至 6.3，并已在设备客户端版本 6.3.1 及更高版本中移除。

此功能允许管理员将便携应用程序和文件内容部署/推送到用户设备的安全存储卷中。一旦设备解锁，终端用户就可以通过应用程序界面中的快捷方式访问内容和应用程序。

在 Windows 上设置网络共享的过程可在 Microsoft 资源中找到。

要发布整个网络共享，请使用以下格式：**\\server-name\network_share**

要在网络共享中发布文件夹，请使用以下格式：**\\server-name\network_share\发布的文件夹**

请注意，网络共享需要尾部的反斜杠，而文件夹不需要。

以下配置可用：

- 启用发布者-内容分发
    - 发布者可让您将内容传递到设备。
- 发布者根文件夹的 UNC 路径
- 需要与 SafeConsole 建立实时连接或位于受信任设备网络中。
    - 启用后，离线状态下或在受信任网络之外时，驱动器将不会同步文件。

策略设备用户交互(客户端 4.8)

设备软件将在设备 UI 上为发布文件夹的每个子目录添加一个按钮。在初始下载过程中，主菜单会显示一个进度条：

- 如果找到名为 safestick.ini 的文件，将使用该文件来配置按钮。语法请参见下文。
- 如果找到带有嵌入描述的可执行文件，将使用该描述作为按钮标题，按下按钮将启动应用程序。
- 如果文件夹只包含一个文件，则文件夹名称将作为按钮标题，按下按钮将使用系统默认操作调用该文件。这仅适用于 4.7 版本之前的设备软件。
- 否则，文件夹名称将作为按钮标题，按下按钮将打开文件夹。

safestick.ini 的语法：

使用 ini 文件，可以为要运行的可执行文件指定参数。

参数可能包含与自定义信息中指定的相同的令牌，因此您可以启动知道从哪个卷或设备启动的应用程序或脚本。

“safestick.ini”文件格式如下：

[starter]

command=<program name>

parameters=<parameters> ; optional

name=<shortcut name>

- 程序名称是要启动的程序的完整路径。要从设备启动程序，请以以下格式输入：{存储路径}\Applications\Program Directory\Program.exe。
- 参数是要传递给程序的任何参数。该值是可选的。
- 快捷方式名称是在设备软件界面中显示的名称。
- 可以通过在单独的行上指定 hidden=yes 来隐藏主菜单中的图标。

策略设备用户交互(客户端 6.2-6.3.1)

当发布者策略被推送到运行 6.2 - 6.3.1 版本的设备时，解锁驱动器后将在设备控制面板上出现一个新的快捷方式。单击此快捷方式将使用户转到位于其驱动器安全分区根目录上的 Publisher 文件夹。此文件夹将包含已发布的文件，每当设备在与发行者策略中定义的文件服务器有有效连接的主机计算机上解锁时，这些文件都会更新。

策略-地址围栏 GeoFence

在策略编辑器弹窗中可用。

如果设备软件尝试从受限 IP 连接，地理围栏（Geofence）将在设备上强制执行拒绝访问状态。一旦设备从非受限网络连接，它将自动恢复正常工作。

为了使地理围栏生效，需要与 SafeConsole 服务器建立实时连接。为了严格执行地理围栏策略，建议使用设备状态策略强制设备始终需要服务器连接进行设备解锁，或者使用 ZoneBuilder 仅允许设备在受信任网络中解锁。

启用地理围栏后，可以将使用限制仅限于指定的国家或 IP。此功能的目的是实现法规遵从性，即不允许数据在指定的国家或 IP 之外传输。

以下配置可用：

- 在设备上启用地理围栏：复选框
  - 通过地理围栏阻止基于用户计算机 IP 地址的设备访问。地理位置数据(例如 IP 地址所在的国家和 ISP)也可以用于控制设备访问。
- 地理围栏对用户的消息：文本框
  - 当用户的设备通过地理围栏策略被拒绝访问时，向用户发送自定义消息。
- IP 地址：文本框。默认情况下，允许所有 IP 地址
  - 使用逗号分隔多个 IP 地址（例如：198.51.100.1,198.51.100.2）。支持通配符和 CIDR 地址（例如：198.51.100.*或 198.51.100.0/24）。
  - 限制模式：单选按钮
    - ✓ 仅允许这些 IP 地址-强烈建议列出已批准的 IP 地址
    - ✓ 限制这些 IP 地址
- 国家：文本框。默认情况下，没有被阻止的国家
  - 限制模式：单选按钮
    - ✓ 仅允许这些国家
    - ✓ 限制这些国家
- ISP：文本框。默认情况下，没有被阻止的 ISP
  - 限制模式：单选按钮
    - ✓ 仅允许这些 ISP
    - ✓ 限制这些 ISP
    - ✓ 要添加 ISP，请点击"添加 ISP"，在弹出窗口中输入与 ISP 关联的已知 IP，并点击搜索符号按钮进行查找，然后在屏幕底部点击"添加"。

策略设备用户交互

当设备被封锁且设备进入拒绝访问模式且无法解锁时，设备软件将显示配置的消息。一旦设备从允许的位

置连接，设备就可以再次解锁。

策略-可信网络

通过提供允许的 IP 地址、国家或 ISP 列表，可以创建可信网络。配置完成后，设备需要连接到一台计算机，该计算机可以通过允许的 IP 地址到达 SafeConsole 服务器，以便将其视为受信任网络和受信任区域的一部分。另一种进入受信任区域的方法是使用 ZoneBuilder 受信任证书。

- 当与 Write-Protection 策略配合使用时，可以确保从不受信任的网络连接时，设备只在只读模式下解锁。
- 当与 ZoneBuilder 策略一起使用时，您可以阻止设备自动解锁，或者在设备从未知网络连接时阻止访问。请注意，您可以使用 ZoneBuilder 证书来安全地信任您受信任网络之外的计算机。

为了使受信任网络（Trusted Network）生效，需要与 SafeConsole 服务器建立实时连接。为了严格执行受信任网络策略，建议使用设备状态策略强制设备始终需要服务器连接进行设备解锁，或者仅允许设备在受信任网络内部使用 ZoneBuilder 进行解锁。

以下配置可用：

- 启用受信任网络：复选框
  - 受信任网络是管理员创建的受信任区域，其他策略可以使用该区域来限制或提供方便的功能，具体取决于设备是在受信任区域内部还是外部解锁。如果未配置受信任网络策略，则所有与 SafeConsole 服务器的实时连接都被视为位于受信任网络中，因此属于受信任区域。为了注册设备，用户需要在受信任网络内部与 SafeConsole 建立连接。
- IP 地址：文本框
  - 使用逗号分隔多个 IP 地址（例如：198.51.100.1,198.51.100.2）。支持通配符和 CIDR 地址（例如：198.51.100.*或 198.51.100.0/24）。
  - 限制模式：单选按钮
    - ✓ 仅允许这些 IP 地址，强烈建议列出已批准的 IP 地址
    - ✓ 限制这些 IP 地址
- 国家：文本框，默认情况下，允许所有国家
  - 输入国家以仅允许这些国家
- ISP：文本框，默认情况下，允许所有 ISP
  - 输入 ISP 以仅允许这些 ISP
  - 要添加 ISP，请点击"添加 ISP"，在弹出窗口中输入与 ISP 关联的已知 IP，并点击搜索符号按钮进行查找，然后在屏幕底部点击"添加"。

策略设备用户交互

当用户试图在可信网络之外注册设备时，会收到警报。其他策略也可以根据用户是否在可信网络内来改变它们与用户交互的方式。一个例子是写保护策略，它可以配置为禁止在受信任区域之外写入设备。在这种情况下，当用户在可信区域外解锁时，将通知他们驱动器是写保护的。

策略-客户端应用程序更新程序

管理员能够将更新推送到 6.2 或更高版本的设备上。每个新的更新必须首先在 Manage Endpoint Updates 部分中得到批准。选择启用客户端应用程序更新程序将自动为列出的所有匹配设备发送更新。

以下是可用的配置：

- 最新版本
  - 此选项将发送最新的设备更新到所有终端
- 指定版本
  - 此选项应与"管理终端更新"部分一起使用。将更新添加到策略后，可以从相应端点旁边的下拉菜单中选择更新。

策略设备用户交互

当设备自动检查更新时，用户将收到有新客户端版本的通知。用户将看到更新的发布说明，并提示在继续之前将数据备份到他们的设备。在更新过程中，用户需要手动允许更新运行，并注意不要通过移除驱动器或计算机电源来中断更新。根据终端的不同，可能需要管理权限。这可以在 Manage Endpoint Updates 部分中查看。

策略-K300/K350/DL4 FE-独立登录

独立模式允许 K300、K350 和 DL4 FE 在不启动解锁客户端的情况下解锁。这使得设备可以通过键盘/触摸屏进行解锁，并且安全卷直接传递给操作系统，使得设备与支持大容量存储设备的任何系统兼容，包括 macOS、Linux 和其他专有系统。当在独立模式下解锁 K300、K350 或 DL4 FE 时，所有管理功能都会暂停，以实现此兼容性。这意味着 SafeConsole 中定义的所有策略都不会生效。然而，如果需要，密码重置仍然有效。独立登录策略是完全可选的，并且默认情况下处于禁用状态。要启用，请按照以下步骤操作：

- 启用独立登录。这将允许设备在未受管理状态下解锁，并在设备以独立模式解锁时禁用所有 SafeConsole 功能。
  - 最大独立登录数：设置最大独立登录数。
  - 自动请求最大独立登录数：当设备在 SafeConsole 模式下解锁时，启动解锁应用程序并与 SafeConsole 建立有效连接时，允许的独立登录数将被重置为最大允许的登录数。

策略设备用户交互

启用后，控制面板中的新设置项将可用。

终端用户将通过点击控制面板中的设置齿轮来请求独立登录，选择独立，输入请求的原因，最后点击请求按钮。请注意，此过程不会影响自动请求活动的设备。

下次在设备上输入密码时，最终用户将被提示选择 STANDALONE 或 SAFECONSOLE。选择"独立"将进入连接菜单，其中可以选择"连接"或"只读模式"将设备连接到主机。选择其中一种模式将直接挂载安全卷，而无需运行 Unlocker 客户端或挂载虚拟 CD 驱动器。如果选择 SAFECONSOLE，则需要在 Windows 操作系统中启动解锁客户端。

每次在设备上选择独立模式并连接到计算机时，独立模式的计数器将减少一。一旦计数器达到零，那么用户将需要在 SafeConsole 中解锁并请求更多登录。

注意：如果文件在独立模式下放置在设备的安全卷上，并且受到防恶意软件或文件限制的 SafeConsole 策略的限制，那么在 SafeConsole 模式下解锁后，文件将被删除。

欲了解更多信息，请参阅以下适用的用户手册：

- K300 用户手册
- DL4 FE 用户手册
- K350 用户手册-尚未发布。

策略-PortBlocker

有关 PortBlocker 的信息，请参阅 PortBlocker 管理指南

危险区域

仅在默认策略编辑器弹窗中可用

危险区域允许管理员将所有路径恢复为默认策略，并将默认策略恢复为出厂设置。此选项应仅作为最后的手段或在 DataLocker 支持的指导下使用。

要启动所有策略的重置，点击危险区域，然后选择"删除并重置所有策略"。这将显示一个弹窗，管理员必须通过输入"删除并重置所有策略"并点击"删除"来确认操作。

审计日志-用户和管理操作

审计日志通过主菜单进入。

在每个子菜单选项的右上方，您可以管理要显示哪些列，并触发将所有注册数据导出为 CSV 或 XML。

用户审核日志

SafeConsole 存储所有设备使用操作的记录。要记录设备审计日志，设备审计策略必须处于激活状态并应用于该驱动器。

驱动器将在脱机时缓冲日志数据，并在连接到 SafeConsole 服务器后传输加密数据。每次解锁驱动器时，驱动器都会执行此操作。

系统消息

所有 SafeConsole 人员的操作都记录在系统消息下。

服务器设置

服务器设置位于主菜单中，用于处理服务器行为。有更多的信息图标，将展开解释每个设置。

这些是服务器设置下可用的选项。

一般

注册和密码重置

- 在注册期间禁用机器所有权确认

默认情况下，在设备注册期间，要求设备用户通过对其计算机用户帐户进行身份验证来验证身份，该用户帐户可以是本地帐户或域帐户。身份验证的目的是确保哪个用户拥有某个设备。身份验证依赖于 NT 用户身份验证，如果此功能不可用，则可以禁用它（需要设备客户端版本 4.8.19+）。

- 对所有设备注册要求使用唯一令牌

对于所有设备注册，用户将需要输入通过 SafeConsole 管理员发起的电子邮件收到的唯一注册令牌（需要设备客户端版本 4.8.25+）。当使用部署向导时，此唯一令牌将与连接令牌和快速连接指南一起发送。管理员还可以通过"用户详细信息"窗口访问该唯一令牌。当使用唯一令牌激活设备时，将使用用户的策略进行设备注册，而不是默认策略。用户的策略需要配置地理围栏 GeoFence 和受信任网络以允许访问。如果用户在地理围栏或受信任网络之外，将阻止注册。注意：此设置关联两个复选框，一个用于设备和 SafeCrypt 驱动器，另一个用于 PortBlocker 终端。

- 要求管理员批准注册

为了避免非组织设备注册到 SafeConsole 服务器的风险，您可以要求 SafeConsole 管理员在完全设备注册完成之前批准。管理员可以在设备的"用户"或"驱动器"下的"操作"菜单中手动批准设备。启用此选项后，可以自定义并在注册过程中向终端用户显示消息。默认消息是："服务器要求批准该设备以完成注册。请联系您的 SafeConsole 管理员了解更多信息。"+要求已注册设备的注册批准。默认情况下，此复选框未

选中。这意味着一旦设备由管理员批准，下次注册时就不需要重新批准。例如，进行出厂重置后。如果您希望每次注册时都批准设备，请选中此选项。

- 为设备和 SafeCrypt 驱动器启用回收站（测试版）

此设置启用了一个回收站，当驱动器被删除时，驱动器将被发送到回收站。在"管理"->"驱动器"部分，可以从回收站恢复驱动器。建议启用此设置，以防止管理员不经意间删除驱动器。

注意：只有 SafeConsole 帐户所有者可以更改此设置。

- 设备密码重置设置：复选框

在密码重置期间，不需要用户向 SafeConsole 工作人员提供设备质询代码。启用此设置后，管理员可以获得任何设备的恢复代码，而无需与设备的用户或所有者进行交互。

- 禁用所有设备审计日志：复选框

启用此设置后，将阻止服务器记录任何设备活动。此设置将覆盖所有配置的策略。

注意：只有 SafeConsole 帐户所有者可以更改此设置。

- 禁用所有系统审计日志：复选框

启用此设置后，将阻止服务器记录服务器上的任何系统或 SafeConsole 管理员活动。

注意：只有 SafeConsole 帐户所有者可以更改此设置。

SMTP 邮件服务器

默认情况下，SafeConsole 从 support@datalocker.com 发送邮件。如果您想更改此设置并使用自己的电子邮件服务器，请选择使用自定义 SMTP 服务器。有关更多信息，请访问：SMTP 帮助。

SafeConsole OnPrem 管理员也可以从 SafeConsole 配置程序配置这些设置。

注意：只有 SafeConsole 帐户所有者可以更改此设置。

自定义邮件模板

这使您能够自定义从 SafeConsole 服务器发送的所有电子邮件。一旦编辑并保存了一条消息，将显示恢复到默认值的选项。要特别注意保持{}内的字符串完整，因为这些是动态字符串，一旦电子邮件发送，它们将被有意义的内容所替换。请参阅下面的图表：

变量	说明
{admin-Email}	发起邮件的管理员邮箱地址

{admin_full_name}	发起邮件的管理员名称
{device}	设备名称
{device-url}	SafeConsole 服务器连接令牌
{display-google-auth}	显示 TOTP 2-Factor 认证消息
{display-sms}	显示 SMS 2-Factor 认证消息
{display-sms-backup}	可下载的 TOTP 备份码
{Email}	收到邮件的用户邮箱地址
{full-Name-add-by}	发起邮件的管理员的名称
{id}	设备序列号
{login-username}	收到邮件的用户登录 SafeConsole 服务器的用户名
{path}	收到邮件的用户路径
{reg-token}	收到邮件的用户的唯一令牌
{reset-url}	一次性重置用户的 SafeConsole 服务器密码链接
{response-code}	密码重置响应码
{site-url}	链接发送邮件的用户所属的 SafeConsole 服务器的地址
{SMS-Phone-number}	设置短信双因素认证时使用的电话号码
{start-url}	允许新添加管理员创建密码的一次性链接
{username}	发送邮件的用户的用户名

可用的自定义电子邮件模板：

- Admin Added：新添加的管理员创建他们的 SafeConsole 帐户的链接

- User Added：包括新添加的用户注册他们的设备的唯一令牌
- 双因素验证：双因素认证已在 SafeConsole 帐户中启用
- 密码重置请求：从密码重置操作弹出窗口发送，给需要设备或终端密码重置的用户一个密码重置响应代码
- SafeConsole 密码重置：用于 SafeConsole 帐户密码重置的链接
- 设备连接指南：包括注册设备到 SafeConsole 的快速入门指南，适用于固件版本 6.0.0+
- 设备连接指南(v4.8.x)：包括注册设备到 SafeConsole 的快速入门指南，适用于固件版本 4.8.x。
- PortBlocker 连接指南：包括将 PortBlocker 端点注册到 SafeConsole 的快速入门指南
- SafeCrypt 连接指南：包括将 SafeCrypt 端点注册到 SafeConsole 的快速入门指南
- SafeConsole 临时密码重置:包括 SafeConsole 管理员的临时密码，该密码将在下次登录时重置。

创建第二个电子邮件模板

如果您想修改使用的电子邮件模板并保留原始模板，单击绿色的"添加新模板"按钮将允许您从头开始创建电子邮件模板。使用唯一的版本名保存此模板，将允许您在下拉框中选择模板版本并将其设置为默认版本。任何设置为默认模板的模板都将在 SafeConsole 中用于相应的操作。

SIEM 集成

外部事件日志记录设置(SIEM 集成)：复选框

SIEM 集成可以将事件日志发送到外部第三方日志监控软件。对 Graylog 和 Splunk 的支持目前处于测试阶段。启用外部事件日志记录后，SafeConsole 管理员可以跟踪、审查并获得发生在 SafeConsole 上的事件通知。可能发生的事件包括但不限于设备被 GeoFence 屏蔽或在用户设备上检测到恶意软件。有关详细信息，请参阅支持文章：外部事件日志记录。

单点登录

单点登录设置(SAML SSO)

单点登录允许管理员使用第三方 SAML 2.0 身份验证轻松登录 SafeConsole。目前，ONELOGIN、PINGONE、PINGFEDERATE 和 OKTA 的支持处于测试版阶段。启用单点登录后，SafeConsole 管理员可以从集中管理的用户存储库进行同步，以便更轻松地进行审查和管理。有关更多信息，请参阅支持文章：单点登录设置。

地理定位 Geolocation

为了在使用本地 IP 时使用地图，现在可以编辑设备报告的地理位置。这使管理员能够更好地了解其组织中的设备使用情况。地理定位需要访问 Google Maps API。如果需要，这可以用矢量图形代替或完全禁用。请注意，禁用谷歌地图并切换到矢量地图只能由 SafeConsole 所有者完成。

管理终端更新

在此部分，将显示与 SafeConsole 管理的设备兼容的新设备更新。建议管理员在将更新添加到允许的策略之前验证所显示版本的发布说明。管理员还应注意哪些更新需要管理员访问权限，以防设备用户无法获得此权限。管理员还可以将更新保存到本地服务器，这样驱动器只需连接到 SafeConsole 服务器即可下载更新。

将设备更新添加到策略中不会推送更新。必须配置策略才能实现此目的。

管理-设置 SafeConsole 管理员

SafeConsole 人员在主菜单选项 Admins 下进行管理。对于 SafeConsole On-Prem 用户，还可以使用安装过程中配置的 AD 安全组来管理访问。这在 SafeConsole On-Prem 安装指南中有介绍。

管理账户配置文件设置

您可以在右上角的下拉菜单中通过小用户图标来管理自己的个人资料设置。选项如下：

- 姓名：编辑您的全名，以在 SafeConsole 管理员页面上显示。
- 电子邮件：更新你的电子邮件地址。
- 登录用户名：更新您的登录用户名。(必须是一个词)
- 手机号码：提供您的手机号码。
- 语言：选择您的语言，或保留系统默认值(英语)
- 主题：选择与您组织的品牌标准一致的配色方案。
- 页面模板：选择 SafeConsole 导航菜单的位置-侧边或顶部
- 空闲超时：输入空闲时间的分钟数，在此时间之后您将注销 SafeConsole

从这个页面中，您还可以选择以下选项卡：

- 更改密码：允许您更新您的密码
- 双因素认证：允许您设置短信 SMS 或谷歌认证双因素认证

- 会话：允许您查看登录会话

管理人员访问级别

SafeConsole 管理员可以预配置三种级别的访问权限：

- 管理员 Administrator 可以购买 license、添加管理员、配置设备、监控审计日志和执行设备操作
- 经理 Manager 可以配置设备、监控审计日志和执行设备操作
- 支持团队 Support 可以执行有限数量的设备操作，例如重置密码。不能更改设备配置。

如果 SafeConsole 所有者启用了自定义角色，则可以添加其他角色。

设置新的管理人员账户

要在 SafeConsole 中设置管理员，请遵循以下步骤：

- 在导航菜单中单击 Admins。
- 单击"添加新人员"：应该打开管理设置窗口。
- 输入管理员的全名和电子邮件地址。
- 选择合适的访问级别：管理员、经理或支持团队。
- 选择合适的帐户安全性，包括密码过期策略和双因素要求。注意：可以为用户设置密码，他们将在第一次登录时被迫更改，或者将通过电子邮件发送密码创建链接给他们。
- 点击添加：创建 admin 用户，并将收到一封欢迎电子邮件，其中包含登录说明。

删除管理人员访问权限

要从"管理员"页面中删除管理员，请从"操作"列中选择"删除"。然后单击 OK 确认管理员删除。管理员将无法再登录 SafeConsole。

注意：如果您只有一个注册管理员，该用户不能被删除。

自定义管理信息显示

修改管理员信息的显示，操作步骤如下：

- 单击"SafeConsole Admins"页面的"列"。
- 在下拉菜单中，选择要显示或删除的数据列。
- 点击远离下拉菜单关闭它。显示的表将根据您的选择进行更新。

导出管理人员信息

要从 SafeConsole 导出管理数据，请遵循以下步骤：

- 在"SafeConsole Admins"页面中单击"导出"。选择以 XML 或 CSV 格式导出数据。
- 将导出文件保存到所需位置

为管理人员设置双因素身份验证

注意：可以强制管理员使用双因素。有关更多信息，请访问此链接：Force 2-Factor

双重身份验证为您的 SafeConsole 管理帐户增加了额外的安全层。要设置双因素身份验证，请遵循以下步骤：

- 单击右上角的用户名，并在下拉菜单中选择配置文件设置。
- 单击"双因素身份验证"选项卡。
- 可能有两种形式的认证。您可以使用短信或基于时间的一次性密码(TOTP)。Google Authenticator 是一个受支持的 TOTP 应用程序。

设置短信的步骤如下：

- 单击左侧的短信图标。
- 输入您的电话号码和国家，然后点击发送代码。
- 输入发送到您手机的令牌，并选择"提交"

通过移动应用程序设置 TOTP，请按照以下步骤操作：

- 单击右侧的 Authenticator 图标。
- 扫描安全码或输入屏幕上显示的密钥到您的移动应用程序
- 输入生成的 SafeConsole 令牌进行确认。

如果同时开启了短信认证和 TOTP 认证，则可以使用任何一种方式登录 SafeConsole。如果失去了对所有身份验证方法的访问权限，那么另一个 SafeConsole 管理员将需要删除并重新添加被锁定的管理员。

启用 web 控制台访问的 Geofence 策略

此设置只能由帐户所有者配置。启用后，将限制哪些 ip、国家或 isp 可以登录 SafeConsole 管理门户。这不会影响检查到服务器的设备。有关更多信息，请参见：Admin Geofence

注：只有 SafeConsole 帐户所有者可以更改此设置。

自定义基于角色的安全设置

为 SafeConsole 管理员提供基于角色的安全支持。角色可以自定义，以仅允许在 SafeConsole Web 门户中执行特定操作和查看特定数据。有关更多信息，请访问：自定义基于角色的安全性。

启用自定义基于角色的安全性后，用户可以晋升为组管理员。此权限将允许该用户访问 SafeConsole，并为同一 OU 路径下的用户提供支持。如果不希望使用此子系统，可以禁用它。有关更多信息，请访问：组管理员推广。

注意：只有 SafeConsole 帐户所有者可以更改此设置。

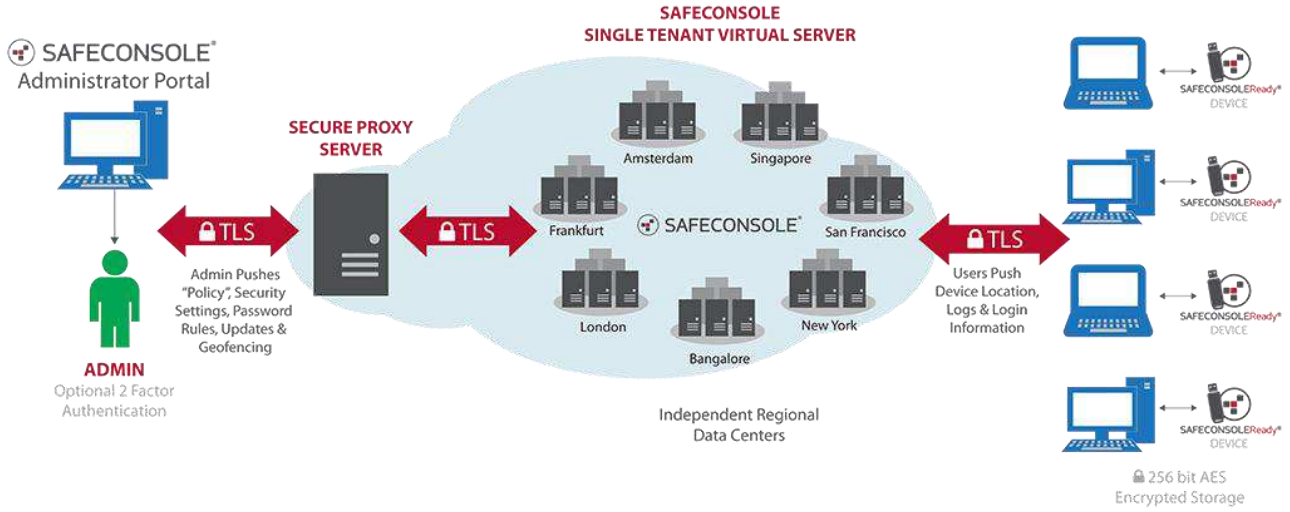
将设备连接到 SafeConsole

当您将设备注册到服务器时，设备将由 SafeConsole 进行管理。

用户可以通过设备软件识别已部署的注册表密钥与 SafeConsole URL 进行注册，或者通过在设备软件中输入连接令牌来将其设备注册到 SafeConsole。连接令牌可以通过 SafeConsole 与快速连接指南一起通过电子邮件发送。

一旦注册，设备将嵌入服务器信息，并可以在任何允许的计算机上使用。

设备通信和设置的流程在 SafeConsole Cloud 和 SafeConsole On-Prem 中是相同的。



驱动器连接要求

- 驱动器需要能够通过配置的端口(TCP 443)使用完全限定域名连接到 SafeConsole 服务器。如果流量通过代理，则应注意验证 SSL 流量没有被代理拦截或终止。
- •出站访问 update.nai.com 的 AV 更新，如果配置。

- •如果配置，访问发布者 windows 共享。

快速将设备连接到 SafeConsole

在"帮助>快速连接指南"下，您将找到有关如何将 SafeConsoleReady 设备注册到服务器的分步说明。

将组织的设备注册到 SafeConsole

注意：可以通过部署注册表项为用户预先填充连接令牌。欲了解更多信息，请参阅 https://datalocker.com/safeconsole/help-registry-deployment。

一旦熟悉了 SafeConsole，就可以将所有设备连接到 SafeConsole。

以下是常用部署方法的示例。

示例 1：设备可以在发给终端用户之前由管理员进行预注册。这有助于管理员确保驱动器配置正确。关于这种方法的更多信息请参考：https://support.datalocker.com/support/solutions/articles/4000106178-pre-registering-devices-in-safeco nsole。

示例 2：终端用户收到设备后，可以对设备进行设置。这样可以减轻管理员在设备部署过程中的部分负担。进入"帮助>部署向导"，输入发送"快速连接指南"的邮箱地址。输入多个电子邮件地址，以逗号分隔或用新行分隔。

新设备注册将使用默认策略的 GeoFence 和可信网络配置，除非在服务器设置中启用唯一令牌。

设备注册故障排除

请确保：

- 设备是一个真正的 SafeConsoleReady 安全 USB 设备。有一些安全的 USB 设备不能被 SafeConsole 管理，一些供应商同时出售这两种类型的设备。在"支持的硬件"区域的"帮助>license"中会显示 license 支持的硬件。
- 许可证已正确安装，并且您有一个可用的席位允许设备连接。
- 如果您激活了服务器设置设备注册批准，您将需要在完成设备注册步骤后，在驱动器或用户下积极批准设备。
- 设备未被其他服务器管理。重新安装服务器时可能会发生这种情况。每次设备出厂重置时，它都可以连接到一个新的服务器。该选项可以在用户默认策略下从设备软件中删除。只要确保你从服务器上重置了你的设备，并且在卸载 SafeConsole 之前应用了这个操作，因为一旦它被删除，就不可能断开与卸载服务器的连接。
- 设备从默认策略中定义的 GeoFence 和可信网络内部到达服务器。

许可证安装

在"许可证信息"页面下，您可以查看和安装许可证。如果没有具有可用席位/插槽的激活许可证，任何设备都不能注册到 SafeConsole。

要安装新的许可证，请单击绿色按钮 install new，输入您的产品密钥，然后单击 Activate。您可能需要单击蓝色的"刷新"按钮，以确保新 license 处于激活状态。

SafeConsole On-Prem 许可证

许可机制依赖于通过 Internet 回调 DataLocker 的中央管理服务器来激活，因此请确保允许这样做。这在 SafeConsole On-Prem 安装指南中有详细说明。

支持

在"帮助>支持"下，您可以找到以下链接：

- 通过在线知识库请求客户支持。
- 本手册
- SafeConsole 发行说明
- 下载最新的设备更新。

请访问 http://support.datalocker.com/以查找最新的资源。

故障排除的最佳实践

- 将您的设备和服务器(仅限 On-Prem)更新到最新版本。
- 确保您可以重现错误。
- 收集包含错误的服务器日志(对于 SafeConsole On-Prem)。
    - 位于./logs/ safconsole -*.log
    - 关于如何收集服务器日志的更多信息可以在此链接中找到。
- 收集设备日志(如适用)。这可以在设备软件运行时按 ctrl+alt+F6 生成。您还可以通过运行 windows key+r 和参数 -log-level 3 来启动具有更详细日志记录的设备软件，例如:g:\Sentry3.exe——log-level 3•在一个好的文本编辑器中查看日志，这些日志乍一看可能很难理解，但有时它会告诉您哪里出了问题，一旦您找到了故障点。如果适用，请查看设备或服务器日志中

对应的时间。

- 搜索 http://support.datalocker.com/，看看是否能找到解决方案。
- 错误的截图或记录通常会更快的解决问题。
- 如果您要通过 DataLocker 发布支持票证，应首先联系您的经销商，因为他们可能能够最快地为您提供帮助。

itbigtec 艾体宝

艾体宝科技有限公司

www.itbigtec.com
sales@itbigtec.com

广州市黄埔区开泰大道30号佳都PCI科技园6号楼

T (+86)400-999-3848

各分部：广州 | 成都 | 上海 | 苏州 | 西安 |
北京 | 台湾 | 香港 | 日本 | 韩国

版本：V1.0 - 22/11/14

网络与安全监控方向
(T: 135 3349 1614)

数据存储/数据智能方向
(T: 155 2866 3362)

获取更多资料

itbigtec.com