|  |  |  |
| --- | --- | --- |
| 作者： | 徐樱樱 | Logo_Beckhoff_Red中国上海市静安区汶水路 299 弄 9-10 号市北智汇园4号楼（200072）TEL: 021-66312666FAX: 021-66315696 |
| 职务： | 技术支持部  | 技术工程师 |
| 日期： | 2020-12-01 |
| 邮箱： | yy.xu@beckhoff.com.cn |
| 电话： |  |

|  |
| --- |
| **程序白名单** |
| **摘 要**： 随着工业4.0的推广，工业控制系统上运行的应用程序越来越多，病毒等非法入侵者更容易运行应用程序，导致工业系统的不安全性。倍福控制器可以通过程序白名单解决方案来防止不信任的应用程序的执行。 |
| **关键字：**应用程序 安全性 程序白名单 |
| **附 件：**

|  |  |  |
| --- | --- | --- |
| 序 号 | 文件名 | 备注 |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

 |
| **历史版本：**

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

 |
| **免责声明：**我们已对本文档描述的内容做测试。但是差错在所难免，无法保证绝对正确并完全满足您的使用需求。本文档的内容可能随时更新，也欢迎您提出改进建议。 |
| **参考信息：** |

**目 录**

[1. 软硬件版本 3](#_Toc57731136)

[2. 程序白名单 3](#_Toc57731137)

[2.1. SRP和Applocker区别 3](#_Toc57731138)

[3. AppLocker设置 3](#_Toc57731139)

# 软硬件版本

嵌入式控制器：CX5130-0125（wes7系统，TwinCAT 3.1 4024）

键盘，鼠标，显示器，DVI线缆

# 程序白名单

病毒等安全系统的攻击者经常伪装自己来骗取用户执行应用程序的运行，而程序白名单主要控制未知或不信任的软件的运行，这样就可以保证设备的正常运行。我们的控制器可以通过SRP和Applocker来实现。

## SRP和Applocker区别

[AppLocker](https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/applocker/what-is-applocker)是Windows 10企业版添加的一个功能，是替代[SRP](https://docs.microsoft.com/en-us/windows-server/identity/software-restriction-policies/software-restriction-policies)（Software Restriction Policies，软件限制策略）的较为复杂的一种应用程序白名单解决方案。经过配置后，[AppLocker](https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/applocker/what-is-applocker)可以通过各种不同的规则（比如应用路径）来阻止进程创建操作，[AppLocker](https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/applocker/what-is-applocker)也可以阻止DLL、脚本代码、MSI安装程序等。

# AppLocker设置

案例目的：通过AppLocker来限制CX51控制器桌面TCPIP.exe程序的运行。

1. 直接使用Win+R组合快捷键打开运行，然后输入secpol.msc并点击OK进入。



1. 进入本地安全策略编辑界面，展开Application Control Policies---AppLocker，AppLocker目录下面包括四个方面的规则，分别是可执行规则，Windows安全程序规则，脚本规则和封装应用规则。



1. 双击Executable Rules，右键选择Create new rule



1. 设置新策略，设置权限，在Action中，是用于设置权限的允许和阻止，本次案例中设置阻止，在User or groups中，可以设置用户权限，本次使用默认的Everyone。

 

1. 设置条件，可以通过指定发布者、路径或文件散列来更精确地指定规则，本次案例中选择Publisher



规则类型说明链接：

<https://docs.microsoft.com/zh-cn/windows/security/threat-protection/windows-defender-application-control/applocker/select-types-of-rules-to-create>

1. 创建拒绝文件，点击Browse,选择TF6310-TCP-IP.exe



1. 除此之外，我们还可以设置规则排除，通过界面中的Add exception来选择排除的条件，通过Add添加排除文件



1. 设置新规则的名字以及描述，设置好之后，点击Create,完成设置



9.重启控制器，再次点击TCP-IP.exe,提示这个应用被锁住。



**上海（ 中国区总部）**

中国上海市静安区汶水路 299 弄 9号（市北智汇园）

电话: 021-66312666 传真: 021-66315696 邮编：200072

**北京分公司**

北京市西城区新街口北大街 3 号新街高和大厦 407 室

电话: 010-82200036 传真: 010-82200039 邮编：100035

**广州分公司**

广州市天河区珠江新城珠江东路16号高德置地G2603室

电话: 020-38010300/1/2 传真: 020-38010303 邮编：510623

**成都分公司**

成都市锦江区东御街18号 百扬大厦2305 房

电话: 028-86202581 传真: 028-86202582 邮编：610016

|  |  |
| --- | --- |
| 请用微信扫描二维码通过公众号与技术支持交流 |  |
| 倍福中文官网：https://www.beckhoff.com.cn/ |
| 倍福虚拟学院：https://tr.beckhoff.com.cn/ |
| 招贤纳士：job@beckhoff.com.cn技术支持：support@beckhoff.com.cn产品维修：service@beckhoff.com.cn方案咨询：sales@beckhoff.com.cn |