# NAC设备(Cisco Clean Access) ：防病毒定义更新配置和故障排除

## 目录



## 简介

本文描述如何配置和排除故障在思科网络准入控制(美洲台)设备的防病毒(AV)定义更新需求，以前叫作思科Clean Access。

## 先决条件

### 要求

本文假设，思科Clean Access，包括Clean Access管理器(CAM)和Clean Access服务器(CAS)，安装并且适当地运作。

### 使用的组件

本文档中的信息根据Cisco Clean Access 3.4和以后。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

## 规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

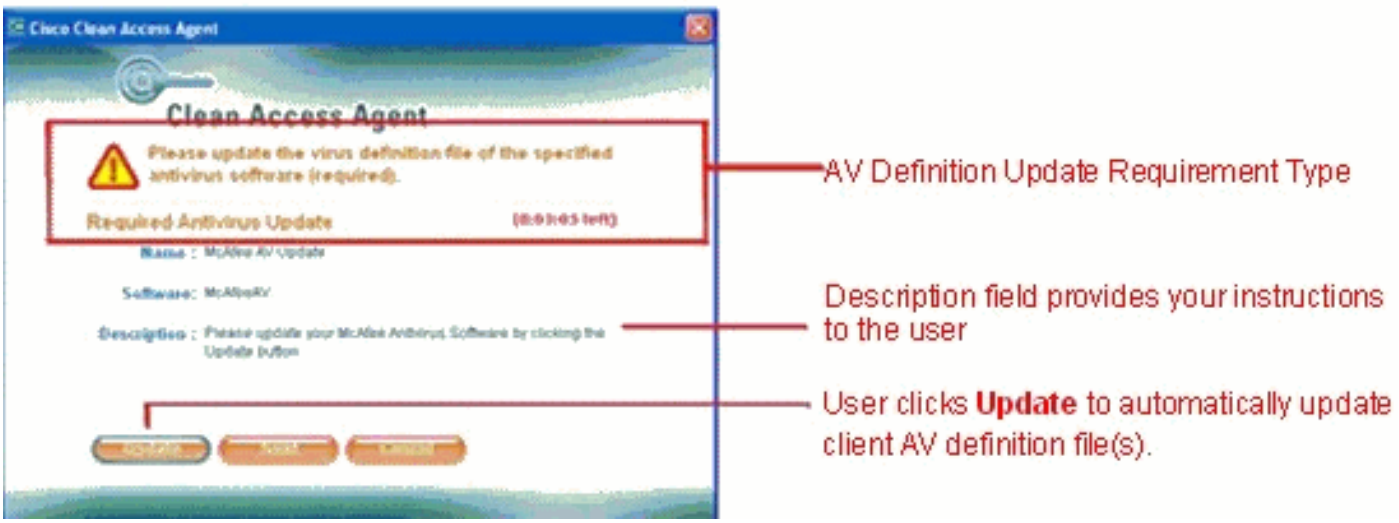
# 配置AV定义更新需求

**AV定义更新**需求类型可以用于为了更新在一个客户端的定义文件支持的防病毒产品的。如果客户端未能会见AV需求， Clean Access代理程序连通直接地与在客户端的已安装防病毒软件和自动地更新定义文件，当用户点击在代理程序对话时的**更新按钮**。

AV规则合并24个防病毒供应商的广泛的逻辑和关联与AV定义更新需求。对于AV定义更新需求，配置类似于那海关规定，除了没有需要配置检查。您连结AV定义更新需求与一个或更多AV规则、用户角色和操作系统并且配置您希望用户发现的Clean Access代理程序对话说明AV需求是否发生故障。

**注意：** 哪里可能，推荐使用AV规则被映射对AV定义更新需求为了检查在客户端的防病毒软件。一旦一种不支持的AV产品、或者，如果AV产品或版本不是可用的通过AV规则，您总是有选项使用思科为防病毒供应商提供了pc_checks和pr_rules或通过**设备管理> Clean Access > Clean Access代理程序**创建他们自己的自定义检查，规则和需求。请使用新的检查、新规则和新的文件/林克/本地检查需求。

此图显示出现的Clean Access代理程序对话，当客户端未能会见AV定义更新需求。




## AV规定

AV规则是预先配置的规则类型被映射对供应商矩阵，并且在支持的AV产品来源的产品列出。没有需要配置与此种规则的检查。

有AV规则两种基本类型：

- **安装AV规则**—此规则证实选定防病毒软件是否为客户端OS安装。
- **病毒定义AV规则**—此规则证实病毒定义文件是否是最新在客户端。病毒定义AV规则可以被映射到AV定义更新需求，以便出故障需求的用户能点击在代理程序的更新按钮为了自动地执行更新

。
AV规则典型地关联与AV定义更新需求。这些步骤要求为了创建AV定义更新需求：

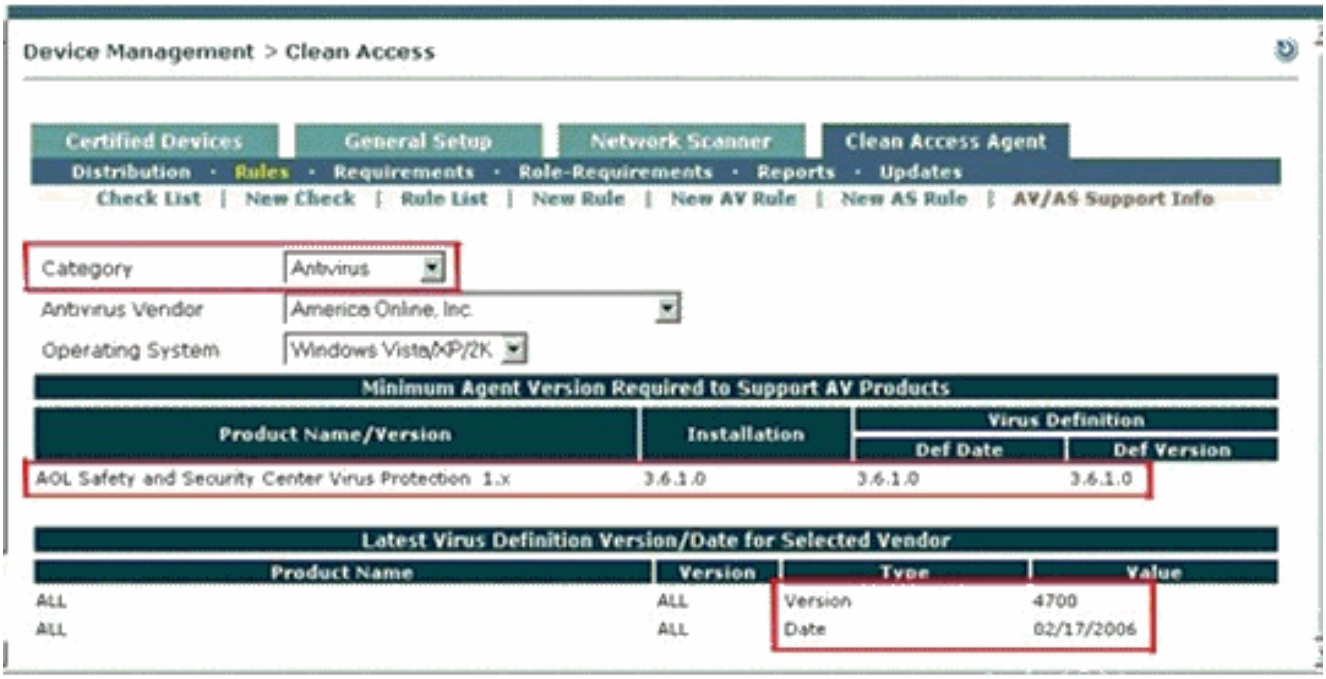
1. 验证AV支持信息
2. 创建AV规则
3. 创建AV定义更新需求
4. 映射需求对规则
5. 应用需求对角色
6. 验证需求

## 验证AV支持信息

Cisco NAC设备允许在网络将使用的Clean Access代理程序的多个版本。当他们发布，对代理程序的新的更新添加最新的防病毒产品的支持。系统选择佳方法， Def伊达市或Def版本为了执行AV根据AV产品联机和代理程序的版本的定义检查。在代理程序兼容性的AV支持info页提供详细信息与最新的支持的AV产品列表下载对CAM。此页列出定义文件新版本和日期每种AV产品的为产品支持需要的代理程序的基准版本。您能对info页AV的支持比较客户端的AV信息为了验证客户端有的定义文件最晚。如果运行代理程序的多个版本在您的网络的，此页可帮助排除故障必须运行哪个版本为了支持特定产品。

完成这些步骤为了查看代理程序支持详细信息：

1. 选择**设备管理> Clean Access > Clean Access代理程序>规则> AV/AS支持资讯台**。
2. 从类别下拉菜单选择**防病毒**。




3. 从下拉菜单选择**防病毒供应商**。
4. 从**操作系统的**下拉菜单选择Windows Vista/XP/2K或Windows 9x/ME为了查看那些客户端系统的支持信息。这填充表如显示：**要求的最低的代理程序版本支持AV产品**—显示要求的最低的代理程序版本为了支持每种AV产品。例如， 4.0.0.0代理程序能登录要求AOL安全中心的病毒防护1.x的角色，但是对于3.6.0.0或更加早期的代理程序，此检查发生故障。如果两Def伊达市和Def版本检查， Def版本检查使用，请注意代理程序支持的版本。**最新的病毒定义版本/伊达市选定供应商的**—显示新版本和日期信息AV产品的。一个最新客户端的AV软件必须显示同样值。

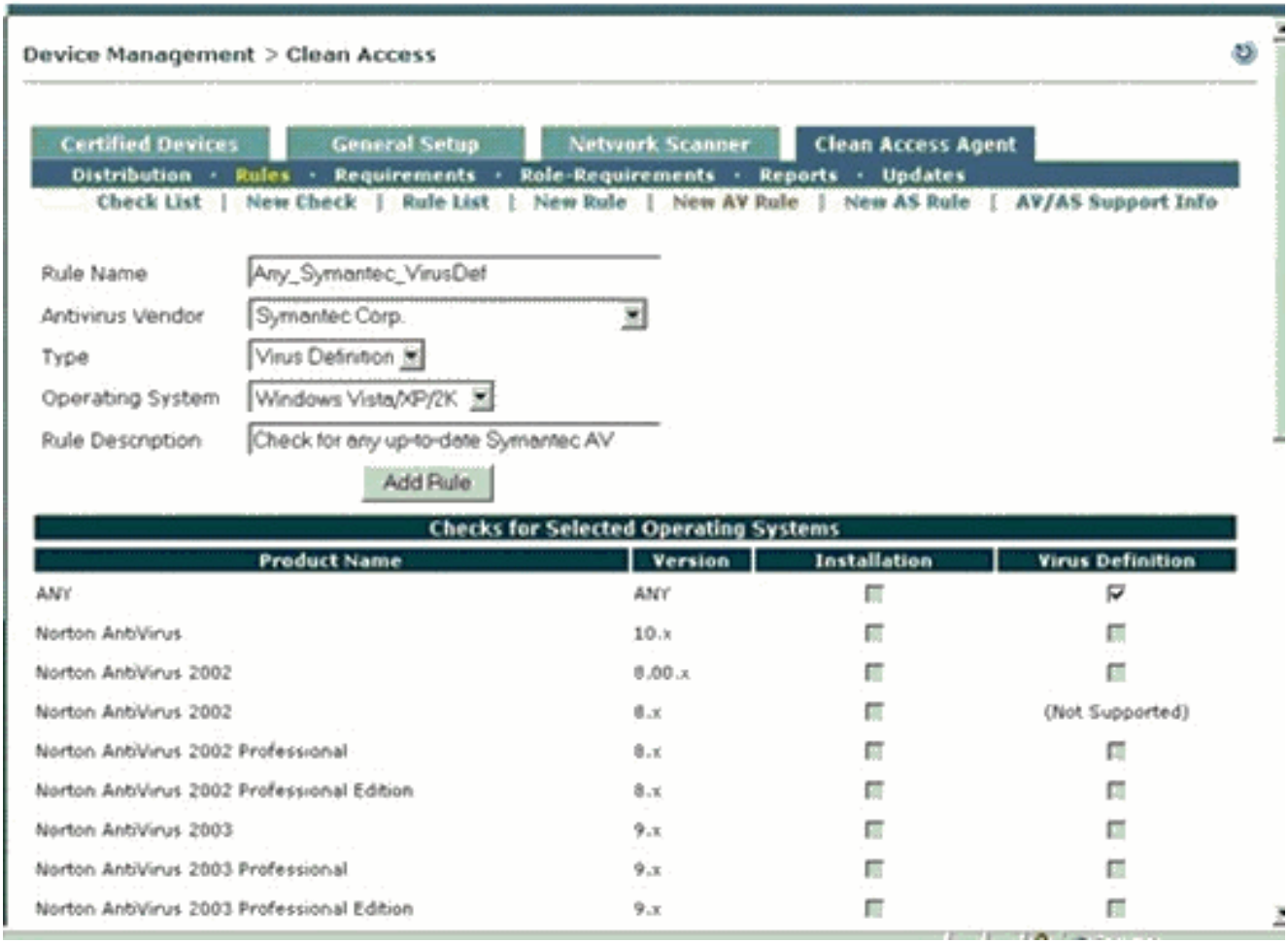
**注意：** 代理程序发送其版本信息对CAM，并且CAM总是尝试首先使用病毒定义版本AV检查。如果版本不是可用的， CAM使用病毒定义日期。

**提示：** 当您从**新的AV规则**表时，选择AV供应商您能也查看最新的定义文件版本。

## 创建AV规则

完成这些步骤为了创建AV规则：

1. 确保您有支持的AV/AS产品列表的新版本。
2. 选择**设备管理> Clean Access > Clean Access代理程序>规则>New AV规则。**

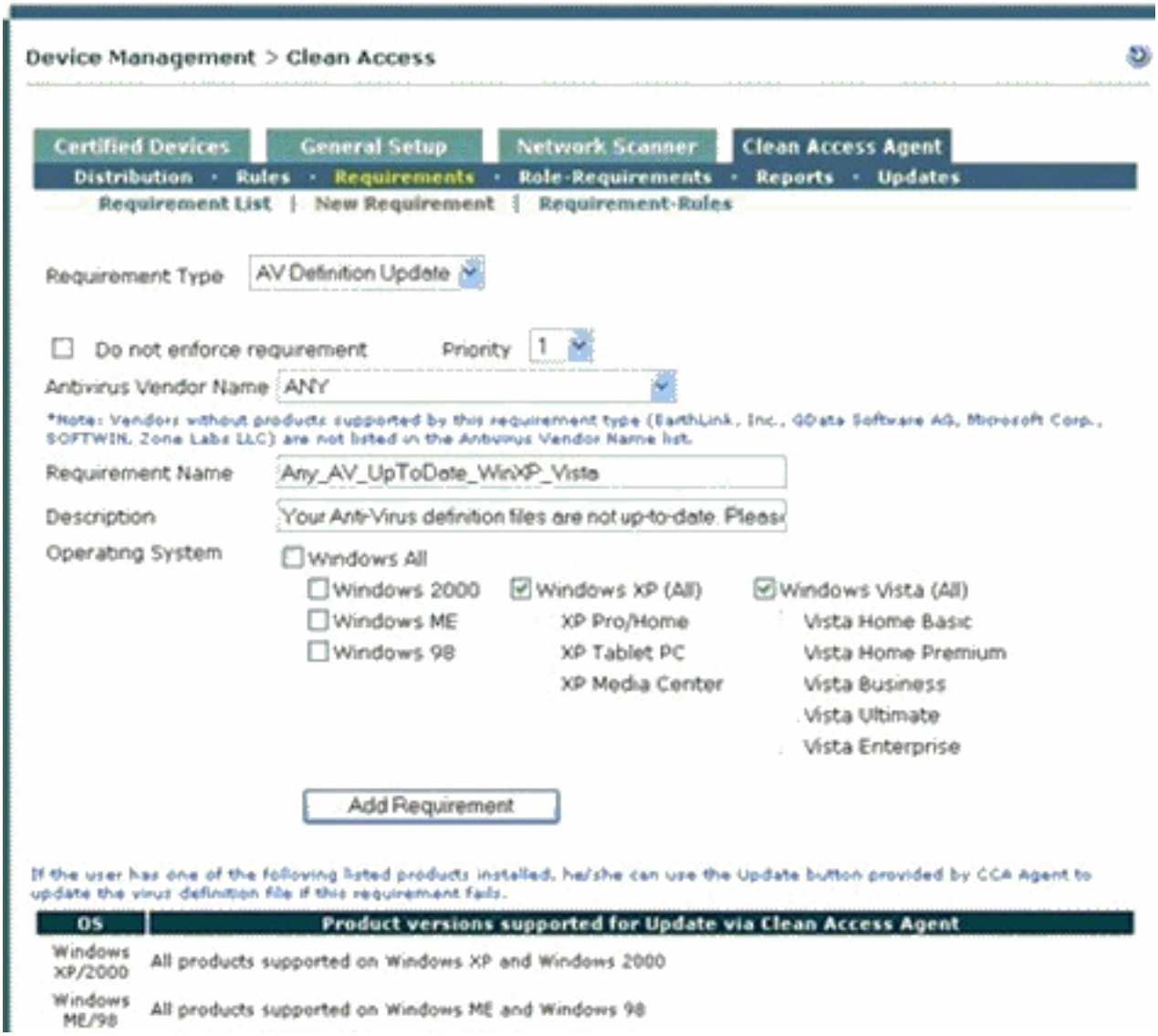



3. 键入**规则名称**。您在名称不能使用位和下划线，但是空间。
4. 从下拉菜单选择**防病毒供应商**。这填充**选定操作系统**表的**检查**在与支持的产品和产品版本的页底端从选定**操作系统的**此供应商。
5. 从**类型**下拉菜单，请选择**安装**或**病毒定义**。这启用对应的安装或病毒定义列的复选框在表里。
6. 从下拉菜单选择**操作系统**， Windows Vista/XP/2K或Windows ME/98。这在表里显示为此客户端OS支持的产品版本。
7. 键入一可选**规则说明**。
8. 在**选定操作系统**表的**检查**，请选择您要检查在客户端的产品版本。为了执行此，请检查在对应的**安装**或**病毒定义**列的一个或更多复选框。**ANY**含义您要检查所有产品和任何版本从此AV供应商。**安装**证实产品是否安装，并且**病毒定义**证实病毒定义文件是否是最新在指定的产品的客户端。
9. 单击**增加规则**。新的AV规则在**规则列表的**底部与您提供的名称的增加。

## 创建AV定义更新需求

这些步骤显示如何创建一个新的AV定义更新需求为了检查客户端系统指定的AV产品，并且与相关的AV的版本规定。如果客户端的防病毒定义文件不最新，用户能单击在Clean Access代理程序的**更新按钮**，并且代理程序造成居民AV软件启动其自己的更新机制。注意实际机制为另外AV产品有所不同，例如，居住更新与line命令参数。

1. 在**Clean Access代理程序**选项卡，请点击**需求**子菜单链路然后**新要求**。



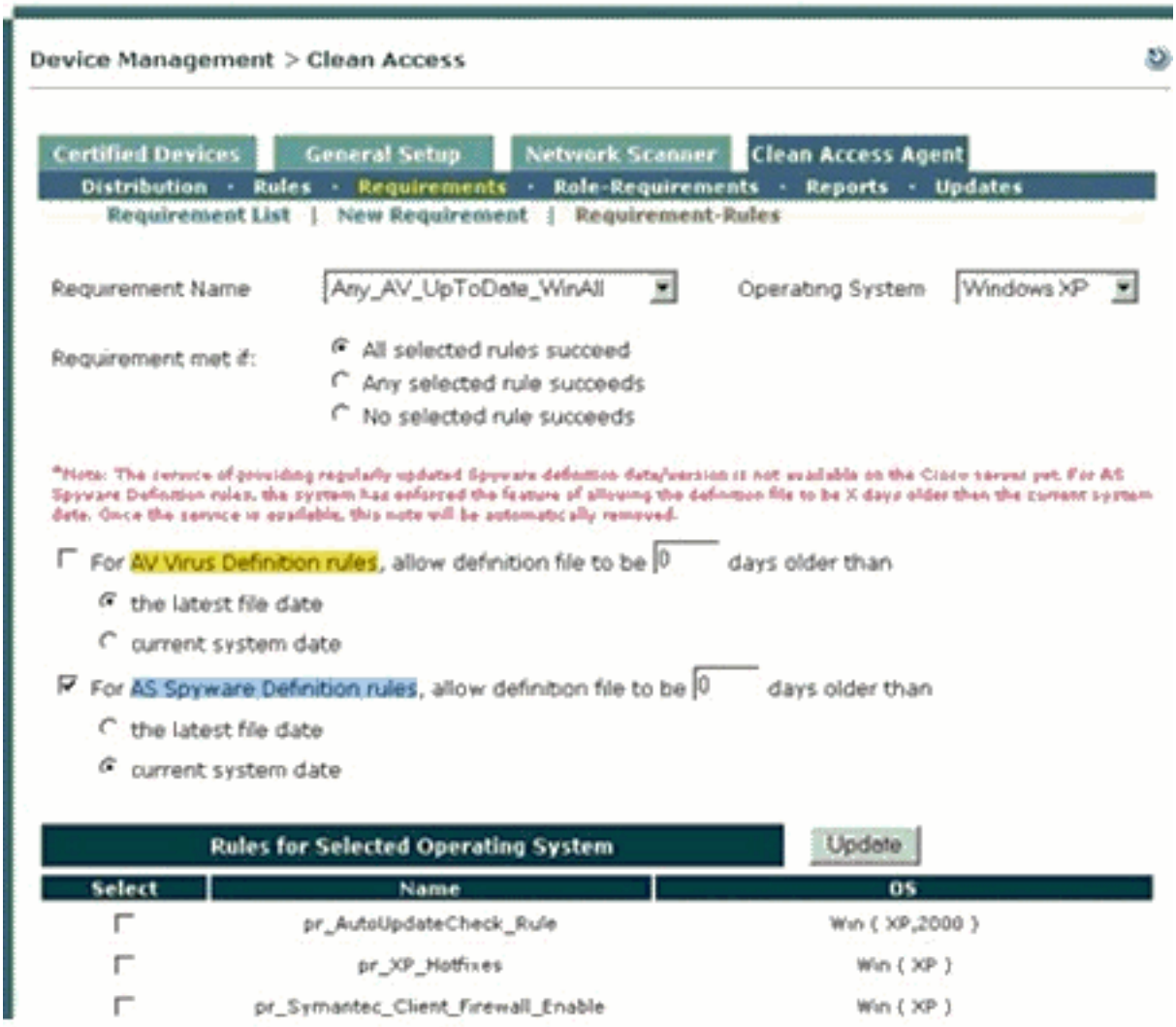

2. 对于**需求类型请**选择**AV定义更新**。
3. 默认情况下请勿**强制执行需求**选项被检查，选定AV定义更新需求如**可选。注意：** 由于Windows更新过程在背景运行，默认情况下请勿**强制执行需求**设置为了优化用户体验。推荐留下此需求，当可选，如果自动地选择下载并且安装选项。WSUS被强制的更新能需要一会儿和启动和在背景的运行。
4. 选择执行**优先级**此需求的在客户端。一高优先级，例如1，含义此需求在代理程序对话被检查在其他需求前的系统并且出现按该顺序。注意，如果强制需求发生故障，代理程序不继续通过该点，直到该需求成功。
5. 从下拉菜单选择**防病毒供应商名称。产品**表列出为每个客户端OS支持的所有病毒定义产品版本。
6. 对于**需求名称**，请键入唯一的名称识别在代理程序的此AV定义文件需求。名称是可视对Clean Access代理程序对话的用户。
7. 在**说明字段**，请键入需求和说明的说明指导未能会见需求的用户。对于AV定义更新需求，您必须包括用户的说明能点击**Update按钮**为了更新他们的系统。记住此信息：**AV定义更新**显示在代理程序的**更新按钮。AS定义更新**显示在代理程序的**更新按钮。Windows更新**显示在代理程序的**更新按钮**。

8. 检查一个或很多这些复选框为了设置需求的**操作系统**：**Windows全部Windows 2000Windows MEWindows 98Windows XP (全部)或一个或很多特定Windows XP操作系统Windows比斯塔(全部)或一个或很多特定Windows比斯塔操作系统**
9. 单击**添加需求**为了添加需求到需求列表。

## 映射需求对规则

一旦需求创建，并且修正链路和说明指定，请映射需求对规则或一套规则。证实的requirement-to-rule映射关联规则集客户端系统是否符合要求对用户需求操作(代理程序按钮、说明，链路)需要为了客户端系统能符合。

1. 在**Clean Access代理程序**选项卡，请点击**需求**子菜单，然后打开**要求规则**表。




2. 从**需求名称**菜单，请选择需求映射。
3. 验证需求的操作系统在**操作系统的**菜单。**选定操作系统的**列表的**规则**带有所有规则可用为选定的OS。
4. 对于AV病毒定义规则(黄色背景)，您能或者配置CAM允许在客户端的定义文件一定数量的天年纪比什么CAM有从**更新的**可得到。请参阅**规则> AV-AS支持资讯台**关于最新的产品文件日期。这允许您配置余地到需求，以便，如果新的病毒定义文件没有从产品供应商发布，您的客户端能仍然通过需求。为此，请完成以下步骤：**比**复选框检查**AV病毒定义规则，允许定义文件是x天年纪**。键入在文本框的一个编号。默认是**0**，指示定义日期大于文件/系统日期不可以。选择以下选项之一：**最新的文件日期**—这大于在CAM的最新的病毒定义日期允许客户端定义文件由您指定几天的数量。**当前系统日期**—这大于CAM系统日期允许客户端定义文件，何时最近一次更新由您指定几天的数量执行。

5. 把页移下来并且在您要与需求产生关联的每个规则旁边检查**Select复选框**。规则在他们的优先级顺序应用，正如此表所描述


:

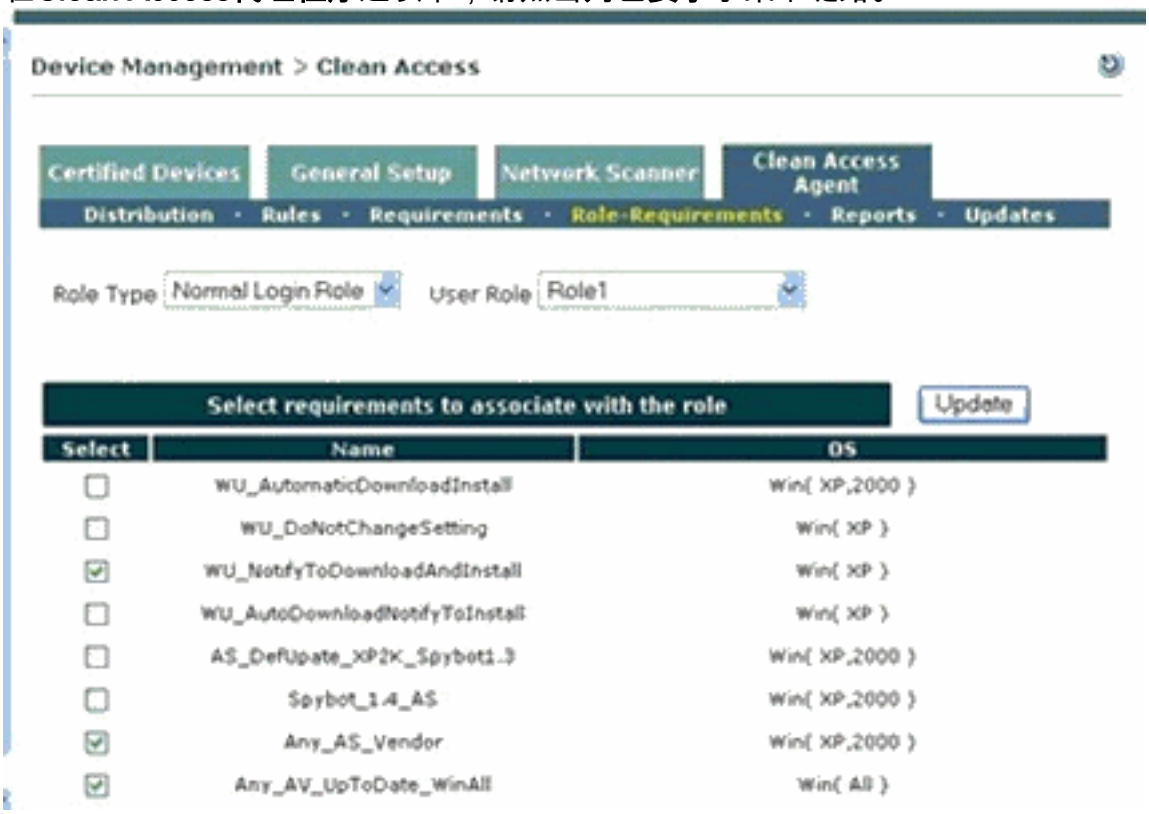
6. **符合的需求，如果**，请选择这些选项之一：—，如果所有规则一定是满足的为了客户端能将考虑与需求一致，**所有选定规则成功**—，如果至少一选定规则一定是满足的为了客户端能将考虑与需求一致，**所有选定规则成功**—，如果必须所有失败为了客户端能认为选定规则与需求一致，**选定规则不成功**如果客户端不是与需求一致，他们必须安装软件关联与需求或完成所需的步骤。
7. 单击**更新**。

## 应用需求对角色

一旦需求创建，配置与修正步骤，并且关联与规则，他们需要被映射到用户角色。此步骤应用您的需求给系统的用户组。

**注意：** 已经确保您安排正常登录用户角色创建。

1. 在**Clean Access代理程序**选项卡，请点击**角色要求**子菜单链路。




2. 从**角色类型**菜单，请选择角色的种类配置。在大多数情况下，这是**正常洛金角色**。
3. 从**用户角色**选择角色的名称菜单。
4. 检查**Select复选框**您要应用对角色的用户的每个需求。
5. 单击**更新**。

6. 在您完成前，请确保角色的用户要求使用Clean Access代理程序。

## 验证需求

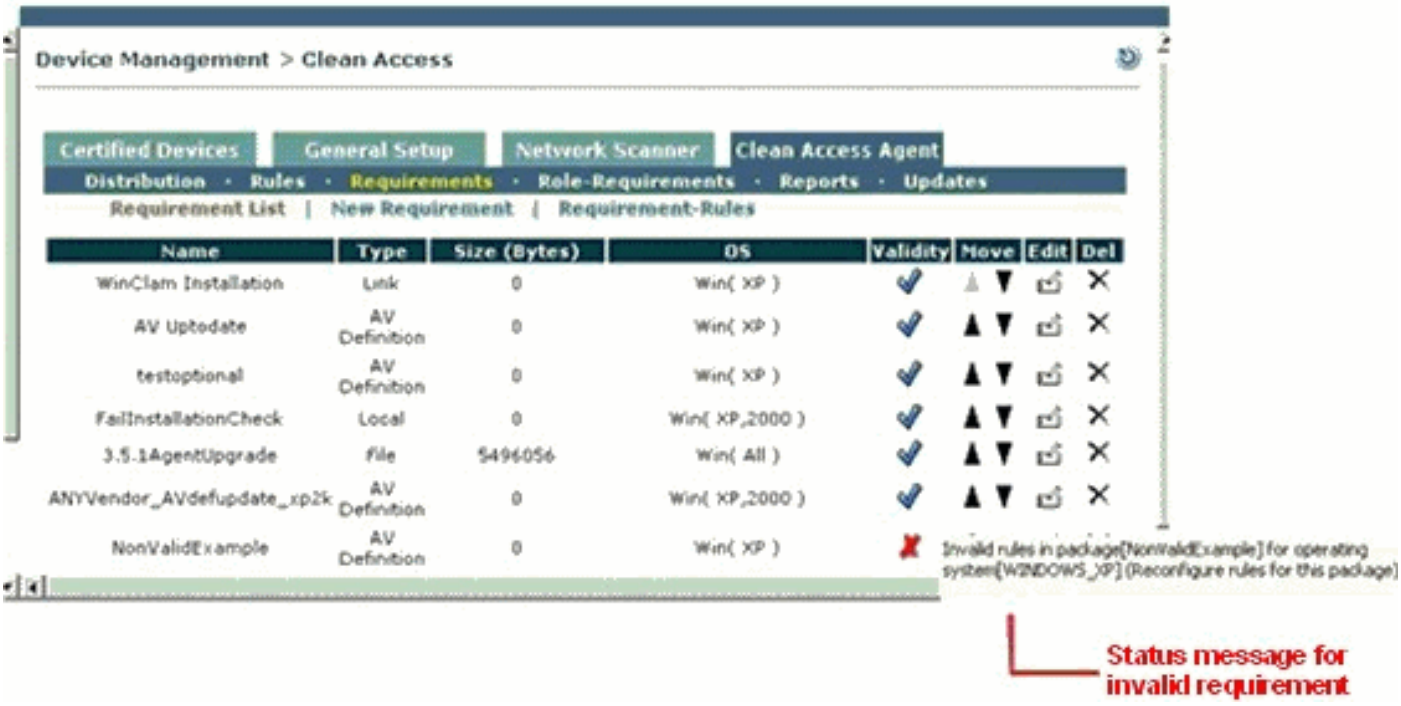
当他们创建， Clean Access管理器自动地验证需求和规则。在**设备管理> Clean Access > Clean Access代理程序>需求>需求列表下的正确性**列显示需求正确性，如显示：

- —需求有效。
- —需求无效。突出显示此图标用您的鼠标按顺序显示此需求的正确性状态消息。规定，并且检查原因需求无效的状态消息状态，此格式的：`Invalid rule [rulename] in package [requirementname] (Rule verification error: Invalid check [checkname] in rule expression)`

在可以使用前，必须更正和使需求有效。一般，当有一操作系统的不匹配时，需求和规则变得无效。

为了更正一个无效需求，请完成这些步骤：

1. 选择**设备管理> Clean Access > Clean Access代理程序>需求>要求规则。**
2. 更正所有无效规则或检查。
3. 从下拉菜单选择无效**需求名称。**
4. 选择**操作系统。**
5. 请确保**符合的需求，如果**：表达式正确地配置。
6. 确保为需求选择的规则有效，含义他们有一个蓝色复选标记在正确性列。




## 思科规则

规则是一个条件语句由一个或更多检查做成。规则与逻辑运算符结合检查为了形成能测试客户端系统的多个功能的一个布尔型语句。

Cisco NAC设备提供一套预先配置的规则，并且检查通过更新连接。已经预配置规则有PR前缀在他们的名称，例如`pr_AutoUpdateCheck_Rule`。请参阅思科预先配置的规则(“pr_”)欲知更多信息。

## 思科检查

检查是检查客户端系统功能，例如文件、注册表项、服务或者应用程序的一个条件语句。已经预配置检查有前缀在他们的名称，例如pc_Hotfix828035。此表列出检查联机种类，并且什么他们测试。

| 检查类别 | 检查类型 |
| --- | --- |
| 注册检查 | • 注册表项是否存在<br>• 注册表项值 |
| 文件检查 | • 文件是否存在<br>• 修改或创建日期<br>• 文件版本 |
| 服务检查 | • 服务是否运作 |
| 应用程序检查 | • 应用程序是否运行 |

## 思科预先了配置规则(“pr_ ")

Cisco NAC设备提供一套预先配置的规则，并且下载对CAM通过在CAM Web控制台的**更新**页的检查，在**设备管理> Clean Access > Clean Access代理程序下>更新**。

已经预配置规则有PR前缀在他们的名称，例如pr_XP_Hotfixes，并且复制为使用作为模板，但是不可能编辑或删除。您能点击所有pr_规则的**编辑按钮**为了查看定义了它的规则表达式。一个预先配置的规则的规则表达式撰写预先配置的检查，例如pc_Hotfix835732和布尔运算符。预先配置的规则的规则表达式通过思科更新更新。例如，当新的关键Windows OS ICM Hotfixes为Windows XP时发布，pr_XP_Hotfixes规则更新与相关ICM Hotfixes检查。

已经预配置规则是列出的在**设备管理> Clean Access > Clean Access代理程序>规则>规则列表下**。已经预配置检查有前缀在他们的名称并且是列出的在**设备管理> Clean Access > Clean Access代理程序>规则>核对清单下**。

**注意：** 思科预先了配置规则打算为仅关键Windows OS ICM Hotfixes提供支持。

# 故障排除

本部分提供了可用于对配置进行故障排除的信息。

## 思科Clean Access不更新客户端的AV定义

要解决此问题，请执行以下步骤：

1. 在CAM中，请选择**设备管理> Clean Access >需求>要求规则**。
2. 取消选定预先配置的规则(pr_)，如果其中任一。
3. 选择适当的AV规则。

## 无法的CCA检测AV

如果怀疑CCA不检测或认可某些AV检查，您需要运行在客户端的OESIS诊断工具。

完成这些步骤：

1. 启用日志记录。注册Clean Access代理程序关于关于如何的说明的参考的Enable (event)调试启用注册客户端的调试。
2. 尝试登陆。
3. 运行OESIS诊断工具。
4. 禁用记录日志。

**注意：** 如果能获取注册表项结构的出口从AV产品的，通常查找在HKLM \软件\ <av_vendor>，也是有用。

## 相关信息

- Cisco NAC Appliance (Clean Access)支持页面
- 技术支持和文档 - Cisco Systems