Websense Manager 帮助

Websense® Web 安全
Websense Web Filter

v7

10240 Sorrento Valley Rd., San Diego, CA 92121, USA

Published 2008
Printed in the United States and Ireland

Trademarks

目录

1 开始

无论是商业、教育、政府或是其他机构所有领域的网络管理员均能利用 Websense 软件轻松控制或监视 Internet 网络流量。

- 这样就可将员工因访问不雅、不当或与工作无关的 Internet 数据而浪费的工作时间降至最低。
- 同时能够最大限度地减少网络资源的滥用情况和因不当访问而导致的法律诉讼。
- 还可为您的网络增加稳固的安全系统，保护网络不受潜在的间谍软件、恶意软件、黑客活动和其他入侵的威胁。

从这里您可以了解下列项目的有关信息：

Websense 基本配置	**执行 Internet 筛选功能**
• *使用 Websense Manager*，第 16 页 • *您的订购*，第 25 页 • *Websense 主数据库*，第 28 页 • *验证 Network Agent 配置*，第 295 页	• *筛选类别与协议*，第 34 页 • *添加客户端*，第 59 页 • *使用策略*，第 64 页 • *将策略分配给客户端*，第 68 页

您还可以了解如何：

评估您的配置	**改善筛选策略**
• *今天：从子夜以来的运行状况、安全和数值情况*，第 20 页 • *历史：最近 30 天*，第 23 页 • *演示报告*，第 84 页 • *调查报告*，第 100 页 • *工具箱可用于验证筛选行为*，第 166 页	• *创建自定义类别*，第 150 页 • *针对特定站点重新定义筛选*，第 153 页 • *限制用户只能访问已定义列表中的 Internet 站点*，第 141 页 • *根据关键字筛选*，第 151 页 • *根据文件类型管理通信*，第 163 页 • *使用 Bandwidth Optimizer 来管理带宽*，第 161 页

概述

Websense 软件和代理服务器、防火墙、路由器和缓存设备等集成设备配合使用，可为您提供相关引擎和配置工具，以帮助您制订、监视和执行 Internet 访问策略。

同时，一系列 Websense 组件（具体描述参见 *Websense 产品组件*，第 226 页）还提供 Internet 筛选、用户识别、警报、报告和故障排除功能。

本 Websense 软件版本包括的新功能概述可参阅 Websense 支持门户中的发布说明。

安装后， Websense 软件将应用**默认**策略在不阻止请求的情况下监视 Internet 的使用情况。除非您定义自己的策略并将它们分配给客户端，否则此策略将控制网络中所有客户端的 Internet 访问。即使您已创建自定义的筛选设置，若客户端不受任何其他策略控制，则 “默认” 策略仍然适用于该客户端。请参阅*默认策略*，第 64 页，以了解更多信息。

有关创建筛选器、添加客户端、定义策略和在客户端应用策略的流程描述，请参阅：

- *Internet 使用情况筛选器*，第 33 页
- *客户端*，第 51 页
- *Internet 筛选策略*，第 63 页

Websense Manager 是一种基于浏览器的单一工具，它可为您提供进行常规配置、策略管理的中心图形界面和 Websense 软件的报告功能。请参阅 *使用 Websense Manager*，第 16 页，以了解更多信息。

您可定义 Websense Manager 的访问级别，使某些管理员仅能管理特定的客户端组，或使某些个人可以运行其各自的 Internet 使用报告。请参阅*委派管理*，第 197 页，以了解更多信息。

使用 Websense Manager

相关主题：

- *登录 Websense Manager*，第 17 页
- *Websense Manager 导航*，第 19 页
- *今天：从子夜以来的运行状况、安全和数值情况*，第 20 页
- *历史：最近 30 天*，第 23 页

Websense Manager 是一种中心配置界面，可用于自定义筛选行为、监视 Internet 使用情况、生成 Internet 使用报告，以及管理 Websense 软件的配置和设置。以下两种浏览器支持运行这款基于 Web 的工具：

- Microsoft Internet Explorer 7
- Mozilla Firefox 2

尽管使用其他浏览器可能也可以启动 Websense Manager，但只有使用支持的浏览器才能发挥其全部功能并正常显示应用程序。

要启动 Websense Manager，请执行下列指示之一：

- 在 Windows 计算机上：
  - 转到**开始 > 所有程序 > Websense**，然后选择 **Websense Manager**。
  - 双击 Websense Manager 桌面图标。
- 在您的网络中任意一台联网计算机上打开支持的浏览器，并输入以下内容：

  `https://<IP 地址 >:9443/mng`

  将 *<IP 地址 >* 替换成 Websense Manager 计算机的 IP 地址。

如果无法连接默认端口上的 Websense Manager，请参考 Websense Manager 计算机默认路径为 **C:\Program Files\Websense\tomcat\logs** 或 **/opt/Websense/tomcat/logs/** 上的 **tomcat.log** 文件以验证端口是否正确。

如果使用的端口正确，但仍然无法从远程计算机连接 Websense Manager，请确保您的防火墙是否允许该端口的通讯。

SSL 连接可实现与 Websense Manager 间基于浏览器的安全通讯。此连接使用 Websense, Inc. 颁发的安全证书。由于支持的浏览器无法将 Websense, Inc.，识别为已知的认证机构，因此在新浏览器中初次启动 Websense Manager 时会显示证书错误。为避免显示此错误，可在浏览器中安装证书或永久性接受证书。请参阅 Websense 知识库以了解更多信息。

安全证书一经接受，浏览器窗口将显示 Websense Manager 登录页面（请参阅 *登录 Websense Manager*）。

登录 Websense Manager

相关主题：

- *使用 Websense Manager*
- *Websense Manager 导航*，第 19 页
- *今天：从子夜以来的运行状况、安全和数值情况*，第 20 页
- *历史：最近 30 天*，第 23 页

安装后，登录 Websense Manager 的首个用户将获得全部管理访问权限。该用户名为 **WebsenseAdministrator**，且不可更改。WebsenseAdministrator 的密码会在安装期间自动配置。

要登录，请先启动 Websense Manager （请参阅*使用 Websense Manager*）。在登录页面上：

1. 选择一个 **Policy Server** 进行管理。

   如果您的操作环境仅包括一个 Policy Server，则它将被默认选中。

2. 选择一个**帐户类型**：
   - 要使用 Websense 用户帐户登录，例如 WebsenseAdministrator，请单击 **Websense 帐户**（默认）。
   - 要使用网络凭据登录请，单击**网络帐户**。
3. 请输入**用户名**和**密码**，然后单击**登录**。

您已登录进入 Websense Manager。

- 如果您首次登录 Websense Manager，系统会提供启动快速入门教程的选项。如果您不熟悉 Websense 软件，或者不熟悉此版本的 Websense 软件，我们强烈建议您学习快速入门教程。
- 如果您使用的是委派管理，而且已创建管理角色，系统可能会提示您选择要管理的角色。请参阅*委派管理*，第 197 页，以了解更多信息。

Websense Manager 会话将在用户界面中的最后一次操作（切换页面、输入信息、缓存更改或保存更改）之后 30 分钟终止。会话终止前 5 分钟将显示警告消息。

- 如果该页面上存在未缓存更改或是未决的已缓存更改，会话终止时这些更改将丢失。请务必单击**确定**以执行缓存，然后单击**全部保存**以保存并执行任何更改。
- 如果在同一个浏览器窗口的多个选项卡中打开了 Websense Manager，所有实例将共享同一个会话。如果一个选项卡中的会话超时，则该会话在所有选项卡中都将超时。
- 如果在同一台计算机上的多个浏览器窗口中打开了 Websense Manager，所有实例将共享同一个会话**如果**：
  - 您使用的是 Microsoft Internet Explorer，并用 Ctrl-N 快捷方式打开新的 Websense Manager 实例。
  - 您使用的是 Mozilla Firefox。

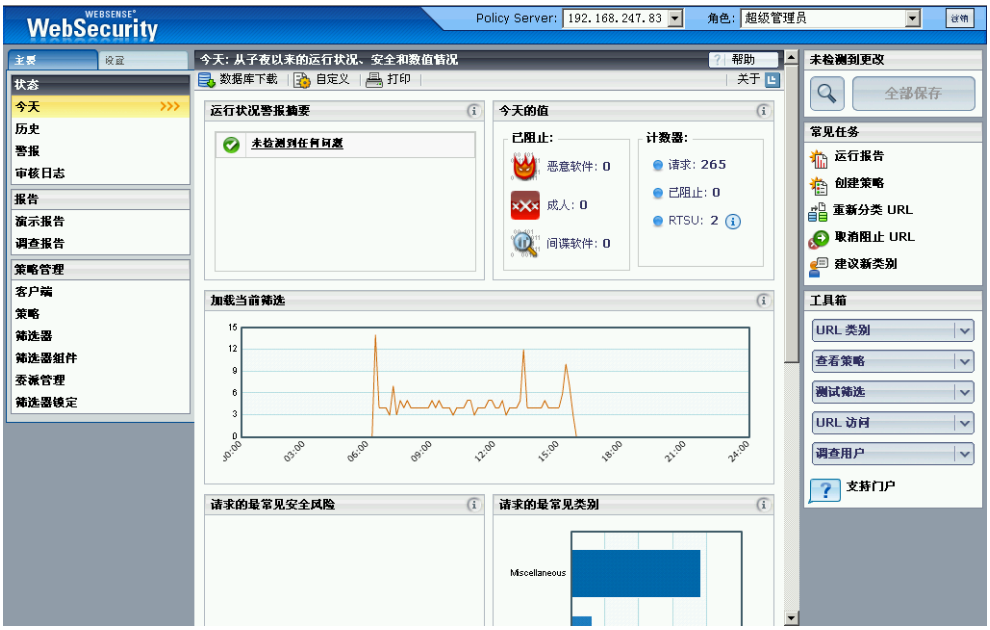
  如果一个窗口中的会话超时，则该会话在所有窗口中都将超时。
- 如果您启动的多个 Internet Explorer 窗口相互独立，并以不同的 Websense Manager 管理员身份使用这些窗口进行登录，则这些窗口**不会**共享一个会话。如果一个窗口超时，其他窗口将不受影响。

如果您未注销 Websense Manager 就关闭浏览器，或者您用来访问 Websense Manager 的远程计算机意外关闭，您可能会被暂时锁定。Websense 软件可在 2 分钟内检测到此问题并终止已中断的会话，使您能够重新登录。

Websense Manager 导航

Websense Manager 界面可分为 4 个主要区域：

1. Websense 横幅窗格
2. 左侧导航窗格
3. 右侧快捷窗格
4. 内容窗格



Websense 横幅窗格显示：

- 您当前登录的 **Policy Server**（请参阅*与 Policy Server 协同工作*，第 231 页）
- 您当前的管理**角色**（请参阅*管理角色概述*，第 197 页）
- **注销**按钮，以便您终止管理员会话

Websense Manager 显示的内容依登录用户所具有的权限而异。例如，用户如果只有报告权限，就无法看到服务器配置设置或策略管理工具。请参阅*委派管理*，第 197 页，以了解更多信息。

本部分描述的选项可供 WebsenseAdministrator 以及其他享有超级管理员权限的用户使用。

左侧导航窗格有两个选项卡：**主要**选项卡和**设置**选项卡。**主要**选项卡可用于访问状态、报告和策略管理功能。**设置**选项卡可用于管理 Websense 帐户，以及执行全局的系统管理任务。

右侧快捷窗格包含实用工具和常用管理任务的链接。在这里还可以查看和保存您在 Websense Manager 所作的任何更改。

- 导航窗格的顶部将显示是否有需要保存的已缓存更改。使用 Websense Manager 时，“更改”栏将指出是否有**未决更改**。

大多数情况下，当您在 Websense Manager 中执行任务并单击**确定**时，您的更改就已缓存。（有时您必须在次级页面和主页面上都单击“确定”才能缓存更改。）

缓存更改后，单击**全部保存**以保存并执行更改。要在保存之前查看已缓存的更改（请参阅*查看、保存和放弃更改*，第 20 页）。请单击**查看未决更改**按钮。该按钮位于“全部保存”左侧。

- **常见任务**为用户提供访问常用管理任务的快捷方式。单击列表中的某一项即可跳转至执行该任务的页面。
- **工具箱**中含有方便易用的快速查找工具，可用于验证筛选设置的有效性。请参阅*工具箱可用于验证筛选行为*，第 166 页，以了解更多信息。

查看、保存和放弃更改

当您在 Websense Manager 中执行任务并单击**确定**时，您的更改就已缓存。使用**查看未决更改**页面可查看已缓存的更改。

重要

请避免在“确定”按钮上重复点击。在同一个按钮上迅速多次点击会导致 Mozilla Firefox 出现显示问题，只有退出并重新打开浏览器才能解决。

对单一功能区所作的更改一般会被归为缓存列表中的单一条目。例如，如果您添加 6 个客户端并删除 2 个客户端，缓存列表仅会显示对“客户端”进行了更改。而对单一“设置”页面所作的更改则可能导致缓存列表中出现多个条目。这种情况会在单一“设置”页面用于配置多个 Websense 软件功能时出现。

- 要保存所有已缓存更改，请单击**保存所有更改**。
- 要放弃所有已缓存更改，请单击**取消所有更改**。

选择“全部保存”或“全部取消”后，右侧快捷窗格中的“更改”栏将作相应更新，您将返回最后一次选择的页面。“全部保存”和“全部取消”功能无法进行“撤销”操作。

使用“审核日志”可查看在 Websense Manager 所作的更改详情。请参阅*查看并导出审核日志*，第 236 页，以了解更多信息。

今天：从子夜以来的运行状况、安全和数值情况

相关主题：

- *Websense Manager 导航*，第 19 页
- *历史：最近 30 天*，第 23 页
- *自定义“今天”页面*，第 22 页
- *警报*，第 239 页

状态 > 今天：自子夜以来的运行状况、安全和数值情况页面将在登录进入 Websense Manager 后最先出现。它将显示筛选软件的当前状态，并图解显示自凌晨 12:01 （根据日志数据库计算机上的时间）开始 24 小时内的 Internet 筛选活动。

在页面顶部的 2 个摘要部分，可为用户提供当前状态的快速概览：

- **运行状况警报摘要**可显示 Websense 软件的状态。如果摘要中出现错误或警告，请单击警报消息，打开 “警报”页面以了解更多详细信息请参阅 *查看当前系统状态*，第 245 页。

  “运行状况警报摘要”中的信息每 30 秒更新一次。

- 在**今天的值**下，可查看 Websense 筛选今天对您的网络进行保护的情况、处理的 Internet 请求总数和其他重要活动总数的示例。

摘要信息下面最多可有 4 个图表可为用户提供筛选活动的信息。这些图表可供超级管理员以及获得 “今天”页面报告查看权限的委派管理员访问查看。请参阅 *编辑角色*，第 213 页。

此类图表中的信息每 2 分钟更新一次。您可能需要向下滚动才能查看所有图表。

图表名称	描述
加载当前筛选	请参阅进入日志数据库的已筛选 Internet 流量数量，它每隔 10 分钟显示一次。
请求的最常见安全风险	找出今天请求最多的安全风险类别，然后确定筛选策略是否已为您的网络提供了正确的保护。
请求的最常见类别	查看今天访问最多的类别。了解有关潜在安全、带宽或生产力问题的高级别概况。
按照风险级别加强策略	查看今天已经对每个风险级别允许和阻止了多少请求（请参阅 *风险级别*，第 36 页）。评估当前策略是否有效，或是否需要更改。
按照带宽计算的最常见协议	了解今天您的网络中使用带宽最多的协议。使用此信息评估带宽需要和潜在的策略更改需要。
计算机请求安全风险站点	找出今天访问过安全风险站点的计算机。您可能想要查看这些计算机以确保它们没有受到任何病毒或间谍软件的感染。
最常阻止的用户	查看今天发出请求最多的用户，了解与组织的 Internet 使用标准的一致性。
最常见的未分类站点	了解今天访问最多的未经过 Websense 主数据库分类的站点。转至**常见任务 > 重新分类 URL**，将一个站点分配给一个要筛选的类别。

单击任何条形图，以打开含有更多详细信息的调查报告。

页面上将出现三个按钮：

- **数据库下载**，仅限超级管理员使用，可用于打开页面以查看主数据库下载的状态或启动一项下载 （请查阅 *查看主数据库的下载状态*，第 236 页）。

- **自定义**，仅限超级管理员使用，可用于打开页面以帮助您更改页面上所显示的图表（请参阅*自定义“今天”页面*，第 22 页）。
- **打印**，供所有管理员使用，可用于打开“今天”页面上显示图表可打印版本的次级窗口。使用浏览器选项可打印此页面，这样可跳过 Websense Manager 主窗口中的所有导航选项。

在 Internet 活动和筛选图表下面，**Filtering Service 摘要**显示与当前 Policy Server 相关联的每一个 Filtering Service 的状态。单击 Filtering Service IP 地址，以查看关于 Filtering Service 实例的更多信息。

出于安全因素，Websense Manager 会话将在处于非活动状态 30 分钟后终止。但是，您可选择继续监视筛选及警报数据：在“今天”页面底部勾选**持续监视今天、历史和警报状态，防止超时**。这 3 个页面的信息将持续正常更新，直到您关闭浏览器或导航至另一个 Websense Manager 页面为止。

重要

如启用监视选项并在“今天”、“历史”和“警报”页面停留超过 30 分钟，则只需导航其他 Websense Manager 页面即可返回登录页面。

启用此选项后，请务必在 30 分钟超时时限之前保存任何已缓存更改。

自定义“今天”页面

相关主题：

- *今天：从子夜以来的运行状况、安全和数值情况*，第 20 页
- *自定义“历史”页面*，第 24 页

使用**今天 > 自定义**页面可为“状态”>“今天”页面选择最多 4 个图表。只有享有无限制策略权限的超级管理员（包括 WebsenseAdministrator）才能自定义“今天”页面。

您选择的图表将出现在“今天”页面上，以便所有超级管理员和具有相关权限可查看“今天”页面图表的委派管理员使用。请参阅*编辑角色*，第 213 页。

一些图表可能会显示敏感信息，例如用户名或 IP 地址。请确保您选择的图表可适用于所有可能查看它们的管理员。

要选择图表，请勾选或取消勾选图表名称旁边的复选框。完成选择之后，请单击**确定**返回“今天”页面并查看图表。要在不作更改的情况下返回“今天”页面，请单击**取消**。

有关每个图表中所显示信息的简短描述，请参阅*今天：从子夜以来的运行状况、安全和数值情况*，第 20 页。

历史：最近 30 天

相关主题：

- *今天：从子夜以来的运行状况、安全和数值情况*，第 20 页
- *Websense Manager 导航*，第 19 页
- *自定义 “历史” 页面*，第 24 页

使用**状态 > 历史：最近 30 天**页面可帮助您大致了解最近 30 天的筛选行为。页面上的图表每天凌晨 12:01（根据日志数据库计算机上的时间）更新一次，与前一天的数据合并。

图表和摘要表涵盖的确切时间段取决于 Websense 软件筛选的时间长短。在安装 Websense 软件的第一个月，此页面显示自安装迄今的数据。在此之后，报告会涵盖当日之前 30 天内的数据。

页面顶部的**估计值**将显示 Websense 软件节省的大致时间和带宽，以及许多组织所重视类别的已阻止请求摘要。

单击**时间**或**带宽**项目 （“已保存”下面），可了解估计值的计算方式 （请参阅 *节省的时间和带宽*，第 24 页）。您可单击**自定义**以更改估计值的计算方式。

已阻止请求区域将列出许多组织关注的一些类别，并显示时间段内已阻止请求的总数，从而进一步阐明 Websense 软件如何保护您的网络。

由于角色被授予的报告权限不同，委派管理员可能无法查看下面描述的表格。请参阅 *编辑角色*，第 213 页。

此页面还包括最多 4 个带有筛选突出显示的图表。您可能需要向下滚动才能查看所有图表。图表中的信息每天更新一次。单击图表以启动具有更多详细信息的调查报告。

图表名称	描述
请求的 Internet 活动	查看每天进入日志数据库处理的已筛选 Internet 请求数量。
请求的最常见安全风险	了解最近被访问的安全风险类别，然后确定筛选策略是否为您的网络提供了正确的保护。
请求的最常见类别	查看访问最多的类别。了解有关潜在安全、带宽或生产力问题的高级别概况。
最常见的未分类站点	了解访问最多的未经过 Websense 分类的站点。转至**常见任务 > 重新分类 URL**，将一个站点分配给一个要筛选的类别。
按照带宽计算的最常见协议	了解最近您的网络中使用带宽最多的协议。使用此信息评估带宽需要和潜在的策略更改需要。

图表名称	描述
按照风险级别加强策略	查看最近已经对每个风险级别允许和阻止了多少请求（请参阅*风险级别*，第 36 页）。评估当前策略是否有效，或是否需要更改。
最常阻止的用户	查看最常阻止哪些用户 Internet 请求。了解与组织的 Internet 使用标准的一致性。
策略加强摘要	了解有关最近允许的请求、阻止的对安全风险级别中站点的请求和阻止的对其他站点的请求的概况。考虑哪些方面的筛选需要进行更详细的评估。

页面上将出现两个按钮：

- **自定义**，仅限超级管理员使用，可用于打开页面以帮助您更改页面上显示图表的类型，以及更改估算节省值的方式（请参阅*自定义“历史”页面*，第 24 页）。
- **打印**，供所有管理员使用，可用于打开“历史”页面上显示图表可打印版本的次级窗口。使用浏览器选项可打印此页面，这样可跳过 Websense Manager 主窗口中的所有导航选项。

节省的时间和带宽

除了可提高 Websense 筛选提供的安全性之外，它还有助于最大程度地减少由于低效的 Internet 活动而损失的时间和带宽。

“估计值”区域的“已保存”部分可提供时间和带宽的估计节省值。这些值的计算方式如下：

- 节省时间：**每次访问所使用的典型时间**乘以**已阻止的站点数量**。初始化时，Websense 软件使用默认值作为用户查看请求站点时所使用的平均秒数。已阻止站点值表示“历史”页面所涵盖的时间段中已阻止的请求总数。
- 节省带宽：**每次访问的典型带宽**乘以**已阻止的站点数量**。初始化时，Websense 软件使用默认值作为平均网站消耗的平均字节数。已阻止站点值表示“历史”页面所涵盖的时间段中已阻止的请求总数。

请参阅*自定义“历史”页面*，第 24 页，以了解如何更改这类计算中的值以反映您的组织的使用情况。

自定义“历史”页面

相关主题：

- *历史：最近 30 天*，第 23 页
- *自定义“今天”页面*，第 22 页

使用**历史 > 自定义**页面可确定 “状态” > “历史” 页面中显示的图表类型，并确定计算节省时间和节省带宽的方式。

勾选您希望在 “历史” 页面显示的图表名称旁的复选框，最多可选 4 个。如需每个图表的简短描述，请参阅*历史：最近 30 天*，第 23 页。只有享有无限制策略权限的超级管理员 （包括 WebsenseAdministrator）才能自定义 “历史” 页面上的图表。

一些图表可能会显示敏感信息，例如用户名。请确保您选择的图表可适用于所有可能查看它们的管理员。

超级管理员和委派管理员均可自定义计算节省时间和节省带宽的方式。委派管理员可通过在描述节省时间和带宽计算的弹出窗口中单击**自定义**链接以访问这些字段。

请输入平均时间和带宽测量结果以作为计算基础：

选项	描述
每个阻止页节省的平均秒数	请输入您的组织估计用户查看单个页面所使用的平均秒数。 Websense 软件将已阻止的页面数乘以该值，以确定 “历史” 页面上所显示的节省时间。
每个阻止页节省的平均带宽 [KB]	请输入已查看页面所用的平均字节数 (KB)。 Websense 软件将已阻止的页面数乘以该值，以确定 “历史” 页面上所显示的节省带宽。

完成更改后，请单击**确定**返回 “历史” 页面并查看新图表或时间和带宽估计值。要在不作更改的情况下返回 “历史” 页面，请单击**取消**。

您的订购

Websense 订购根据每个客户端的具体情况发放。客户端可以指用户，也可以指网络中的计算机。

购买订购后，我们将通过电子邮件向您提供订购密钥。每个密钥仅限安装一次 Websense Policy Server。如果需安装多个 Policy Server，则每个 Policy Server 都需要一个单独的密钥。

在开始筛选之前，必须输入有效的订购密钥（请参阅*配置帐户信息*，第 27 页）。然后您才能够下载主数据库 （请参阅 *Websense 主数据库*，第 28 页），以启用 Websense 软件筛选客户端。

第一次成功下载数据库后，Websense Manager 将显示您的订购所包括的客户端数量。

Websense 软件将每天维护已筛选客户端的订购表，并每晚清除当天订购表。在上个表格清除后，客户首次提出 Internet 请求时，其客户端 IP 地址将被纪录入此表格中。

当此表格中所列的客户端数量达到订购级别后，之前未列出的客户端的任何 Internet 访问请求将超出订购范围。在这种情况下，根据您配置的设置，超出订购级别的客户端可能被完全阻止访问 Internet，或被授予不经筛选的 Internet 访问权限。同样，当订购过期时，根据此设置，所有客户端将完全被阻止或可进行不经筛选的访问。

要在订购超出限制或过期时配置筛选行为，请参阅*配置帐户信息*，第 27 页。

要在订购接近或超出限制时配置 Websense 软件以发送电子邮件警告，请参阅*配置系统警报*，第 241 页。

已筛选类别的数量取决于您的 Websense 订购。Websense 软件将对购买行为激活的所有类别中的所有站点进行筛选。

通过 MyWebsense 门户管理您的帐户

Websense, Inc. 为您提供客户门户，地址为 www.mywebsense.com，您可通过该门户访问与您的 Websense 软件相关的产品更新、修补程序、产品新闻、评估信息和技术支持资源。

创建帐户时，系统将提示您输入所有的 Websense 订购密钥。这将有助于确保您能访问与您的 Websense 产品和版本相关的信息、警报和修补程序。

一旦拥有 MyWebsense 帐号，如果您由于丢失 WebsenseAdministrator 密码而无法登录 Websense Manager，只需单击 Websense Manager 登录页面上的**忘记密码**即可。系统将提示您登录 MyWebsense，然后提供生成和激活新密码的说明。

重要

当您请求设立新密码时，您在 MyWebsense 门户中选择的订购密钥必须与您在 Websense Manager “帐号”页面中输入的密钥相匹配。

您组织中的多名成员可用同一个订购密钥创建多个 MyWebsense 登录。

要从 Websense Manager 访问 MyWebsense 门户，请转至**帮助 > MyWebsense**。

激活 Websense Web Protection Services™

Websense Web Security 订购包括对 Websense Web Protection Services 的访问：SiteWatcher™、 BrandWatcher™ 和 ThreatWatcher™。一旦这些服务得到激活，它们将保护您组织的网站、品牌和 Web 服务器。

服务	描述
SiteWatcher	如果您组织的网站感染恶意代码，它将发出警报，使您能够迅速采取措施，以保护可能访问此网站的客户、潜在客户和合作伙伴。
BrandWatcher	• 当您组织的网站或品牌受到网络钓鱼或恶意键盘记录软件的攻击时，它将及时发出警报。 • 它还能提供 Internet 安全信息、攻击详细信息和其他与安全相关的信息，以便您能采取措施、通知客户并将其对公共关系的不利影响减至最低。
ThreatWatcher	• 可从黑客的角度提供您组织的 Web 服务器概况，扫描是否存在任何已知漏洞和潜在威胁。 • 可通过基于 Web 的门户向用户报告风险等级并提供建议。 • 有助于有效阻止并预防针对 Web 服务器的恶意攻击。

登录 MyWebsense 门户以激活 Websense Protection Services。 ThreatWatcher 一旦激活，请登录 MyWebsense 访问针对已注册 Web 服务器的威胁报告。

配置帐户信息

相关主题：

- *您的订购*，第 25 页
- *配置数据库下载*，第 30 页
- *使用协议*，第 156 页

使用**设置 > 帐户**页面可输入和查看订购信息，并更改访问 Websense Manager 所使用的 WebsenseAdministrator 密码。WebsenseAdministrator 是管理 Websense 软件的默认主管理帐户。

您也可使用帐户通过 Websense 软件向 Websense, Inc.，匿名发送协议使用数据。此信息可用于更新 Websense — 一个包括 3600 多万 Internet 网站和 100 多个协议定义的数据库集合（请参阅 *Websense 主数据库*，第 28 页，以了解更多信息）。

1. 安装 Websense 软件后，或在任何时候收到新的订购密钥时，您可使用此**订购密钥**字段输入密钥。

   输入新的订购密钥并单击 “确定” 后，主数据库将自动开始下载。

2. 主数据库首次下载完成后，将出现以下信息：

密钥过期	您的当前订购的结束日期。此日期过后，您必须更新订购以继续下载主数据库以及进行网络筛选。
已订购的网络用户	网络内可被筛选的用户数量。
已订购的远程用户	网络外可被筛选的用户数量（要求具有可选的“远程筛选”功能）。

3. 选择**订购过期或超出限制时的阻止用户**以：
   - 在订购过期时阻止所有用户的所有 Internet 访问。
   - 在超出已订购用户数量时阻止相应用户的所有 Internet 访问。

   如未选择此选项，则用户在这种情况下将进行不经筛选的 Internet 访问。
4. 要更改 WebsenseAdministrator 密码，请首先提供当前密码，然后输入新密码并予以确认。
   - 密码长度必须在 4 至 25 个字符之间，需区分大小写，可包括字母、数字、特殊字符和空格。
   - 为 WebsenseAdministrator 帐户创建一个不易破解的密码至关重要。密码长度最少为 8 个字符，至少包括一个大写字母、小写字母、数字和特殊字符。
5. 勾选**将类别和协议数据发送到 Websense, Inc.**，以帮助 Websense 软件收集关于 Websense 定义的类别和协议的使用数据，并将其匿名提交给 Websense, Inc.。

   此使用数据可帮助 Websense, Inc.，不断增强 Websense 软件的筛选功能。

Websense 主数据库

相关主题：
- *实时数据库更新*，第 29 页
- *实时安全更新™*，第 29 页
- *筛选类别与协议*，第 34 页
- *与 Filtering Service 协同工作*，第 235 页
- *查看主数据库的下载状态*，第 236 页
- *可恢复的主数据库下载*，第 236 页

Websense 主数据库可存储为筛选 Internet 内容提供基础的类别和协议定义 （请参阅*筛选类别与协议*，第 34 页）。

- **类别**可用于将具有相似内容的网站进行分类 （根据 URL 和 IP 地址进行识别。）
- **协议**定义可将用于类似目的 （例如传输文件或发送即时消息）的 Internet 通讯协议进行分类。

Websense 软件安装时会安装限制版本的筛选数据库，但最好尽快下载完整版本的主数据库，以启用完整的 Internet 筛选功能。首次下载主数据库时，请在**设置 > 帐户**页面输入订购密钥 （请参阅*配置帐户信息*，第 27 页）。

如果 Websense 软件必须经过代理才能执行下载，也可使用**设置 > 数据库下载**页面配置代理设置 （请参阅*配置数据库下载*，第 30 页）。

下载完整数据库可能需要数分钟时间，甚至可能超过 60 分钟，这取决于 Internet 连接速度、带宽、可用内存和空余磁盘空间等因素。

首次下载后， Websense 软件将根据您制订的计划下载数据库变更（请参阅*配置数据库下载*，第 30 页）。由于主数据库更新频繁，数据库下载将按默认计划每天进行。

如果主数据库最后一次更新的时间已超过 14 天， Websense 软件将停止 Internet 筛选请求。

如果在任何时候您想启动数据库下载，或者查看最近一次数据库下载的状态、最近一次下载的日期或当前数据库的版本号，请访问**状态 > 今天**并单击**数据库下载**。

实时数据库更新

除计划的下载之外， Websense 软件还可根据需要执行数据库紧急更新。例如，实时更新可用于将以前暂时分类错误的网站进行重新分类。这些更新可确保网站和协议能够正确执行筛选功能。

Websense 软件每小时检查一次数据库更新。

最近的更新将列于**状态 > 警报**页面上（请参阅*查看当前系统状态*，第 245 页）。

实时安全更新 ™

除接收标准的实时数据库更新之外， Websense Web Security 用户还可通过 “实时安全更新”在 Websense, Inc. 发布与主数据库相关的安全更新之后立即接收此更新。

“实时安全更新”可为用户提供额外保护层，防止基于 Internet 的安全威胁。这些更新发布后应立即安装，这样可有效减少漏洞，以防止新的网络钓鱼 （身份欺诈）骗局、流氓应用程序和恶意代码感染主流网站或应用程序。

Filtering Service 每 5 分钟检查一次安全更新，不过，由于更新仅在安全威胁发生后才会发送，因此实际的更新将间歇性地进行，并且不会中断正常的网络活动。

使用**设置 > 数据库下载**页面可启用 “实时安全更新”（请参阅*配置数据库下载*，第 30 页）。

配置数据库下载

相关主题：

- *配置帐户信息*，第 27 页
- *Websense 主数据库*，第 28 页
- *查看主数据库的下载状态*，第 236 页

使用**设置 > 数据库下载**页面可制订主数据库自动下载计划，而且还可提供 Websense 软件必须通过的代理服务器或防火墙的重要信息，从而进行数据库的下载。

1. 选择自动下载的**下载天数**。

   您必须每隔 14 天至少下载一次主数据库，才能确保 Websense 软件不间断地持续执行筛选功能。如果您未选择任何下载天数，Websense 软件将在数据库最后一次下载 7 天后自动尝试下载。

   注意
   “实时安全更新”启用时将禁用下载天数（请参阅步骤 3）。而且将每天自动执行下载，以确保安全更新可使用最新的标准数据库。

2. 选择**下载时段的**开始时间（**自**）和结束时间（**至**）。如未选择时间，则数据库将在 21:00（晚 9 点）至 06:00（早 6 点）期间内进行下载。

   Websense 软件将在这一时段内随机选择时间联系服务器。要配置下载错误警报，请参阅*配置系统警报*，第 241 页。

   注意
   下载或更新后，将数据库载入本地内存时 CPU 使用率会达到 90%。

3. (*Websense Web Security*) 选择**启用“实时安全更新”**可使 Websense 软件每 5 分钟检查一次主数据库的安全更新。当检测到安全更新时，该更新将被自动下载。

   “实时安全更新”可迅速保护您的网络，从而防止新的网络钓鱼（身份欺诈）骗局、流氓应用程序和恶意代码感染主流网站或应用程序等威胁。

4. 如果 Websense 软件必须通过代理服务器或代理防火墙（除与 Websense 软件通讯的集成产品之外）访问 Internet 以下载主数据库，请选择**使用代理服务器或防火墙**，然后配置以下项目。

服务器 IP 或名称	请输入代理服务器或防火墙主机的 IP 地址或名称。
端口	请输入数据库下载必须经过的端口号 （默认为 8080）。

5. 如果第 4 步中配置的代理服务器或防火墙需要身份验证才能访问 Internet，请选择**使用身份验证**然后输入 Websense 软件访问 Internet 所使用的**用户名**和**密码**。

> **注意**
> 如果选择 “使用身份验证” ，则必须配置代理服务器或防火墙，以接受明文验证或基本身份验证，从而启用下载。

默认情况下，用户名和密码将进行编码，以和 Policy Server 计算机的位置所设置的字符相匹配。这种编码可通过**设置 > 目录服务**页面进行手动配置（请参阅*高级目录设置*，第 57 页）。

测试网络配置

为启用 Internet 请求筛选， Websense 软件必须能够识别网络中传出和传入计算机的 Internet 通信。使用 Network Traffic Detector 可确保此 Internet 通讯显示在筛选软件中。请参阅*验证 Network Agent 配置*，第 295 页，以了解相关说明。

如果 Traffic Detector 无法查看网络的所有部分，请参阅*网络配置*，第 287 页，以了解配置说明。

Websense 技术支持

Websense, Inc.，始终致力于不断提高客户满意度。如需获知最新的发布信息，请随时访问 Websense 技术支持网站，以访问“知识库”、产品文档或创建支持请求。

www.websense.com/SupportPortal/

工作时间内的在线请求回应时间大约为 4 小时；工作时间以外的请求，我们会在请求后的第二个工作日给予回应。

除此之外，我们还提供电话援助。为确保您获得快速、高效的电话请求回应，请确保您作好以下准备：

- Websense 订购密钥
- 可访问 Websense Manager
- 可访问运行 Filtering Service 和 Log Server 以及数据库服务器（Microsoft SQL Server 或 MSDE）的计算机
- 访问 Websense 日志数据库的权限
- 熟悉您的网络架构，或身边有具备相关知识的人员
- 运行 Filtering Service 或 Websense Manager 的计算机的规格
- Filtering Service 计算机上运行的其他应用程序列表

如遇严重问题，可能需要提供额外信息。

我们在周一至周五的正常工作时间内提供标准电话援助，电话号码如下：

- 美国加利福尼亚州圣地亚哥：**+1 858.458.2940**
- 英国伦敦：**+44 (0) 1932 796244**

请查阅以上所列的支持网站，以了解工作时间和其他支持选项。

日本客户可联系其经销商，以获取最快捷的服务。

2 Internet 使用情况筛选器

相关主题：

- *筛选类别与协议*，第 34 页
- *筛选器使用*，第 42 页
- *配置 Websense 筛选设置*，第 49 页
- *Internet 筛选策略*，第 63 页
- *改善筛选策略*，第 141 页

策略会对用户的 Internet 访问加以控制。一项策略即一项计划，可以告知 Websense 软件如何和何时筛选对网站和 Internet 应用程序的访问。最简单的策略构成如下：

- **类别筛选器**，用于对网站类别采取操作 （允许、阻止）
- **协议筛选器**，用于对 Internet 应用程序和非 HTTP 协议应用操作
- 决定何时执行各项筛选器的计划

基于策略的筛选令您可以为客户端 （用户、组，以及您的网络中的计算机）分配不同的 Internet 访问等级。首先，创建筛选器来确定准确的 Internet 访问限制，然后使用筛选器来建构一项策略。

在首次安装时， Websense 软件会创建一个**默认**策略并在订购密钥输入之后即开始将其用于监视 Internet 请求 （请参阅*默认策略*，第 64 页）。起初，默认策略将允许所有请求。

注意

当您从较早的 Websense 软件版本升级时，会保存现有的策略设置。升级完毕后，请检查您的策略以确保其仍然正确无误。

要对不同客户端分别采用相应的筛选限制，首先对类别筛选器进行定义。您可以定义：

- 一个类别筛选器，阻止访问除商业与经济、教育，以及新闻与媒体类别之外的全部网站
- 第二个类别筛选器，阻止访问除有安全风险和包含成人信息之外的全部网站

- 第三个类别筛选器，监视网站访问但不阻止对其的访问 （请参阅*创建类别筛选器*，第 43 页）

您还可以定义这些类别筛选器附带的内容：

- 一个协议筛选器，阻止对即时消息与聊天、P2P 文件共享、代理回避，以及流媒体协议组的访问。
- 第二个协议筛选器，允许除了与代理回避相关协议之外的全部非 HTTP 协议
- 第三个协议筛选器，允许全部非 HTTP 协议 （请参阅*创建协议筛选器*，第 45 页）

当您定义了一套与贵机构 Internet 访问规程相对应的筛选器之后，就可以将其添加至策略中并应用至客户端 （请参阅 *Internet 筛选策略*，第 63 页）。

筛选类别与协议

Websense 主数据库会将类似网站 （根据 URL 和 IP 地址确定）加以组织并纳入**类别**中。每个类别都拥有一个描述性名称，如成人信息、赌博或对等文件共享。您还可以根据组织的特定需求来为组站点创建自己的自定义类别 （请参阅*创建自定义类别*，第 150 页）。主数据库类别和用户定义类别共同构成了 Internet 筛选的基础。

Websense, Inc.，不会对主数据库中的类别或站点进行价值评判。类别是用于根据订购顾客的需要来创建实用的站点分组。它们不是为了对任何站点、站点组、个人、或发布兴趣的个人加以特征化，也不应据此解释。与之类似， Websense 类别所附的标签只是便捷的简写内容，并非意图传达、也不应被认为是要传达对主题事宜或分类站点的任何观点或态度、赞同或反对。

主数据库类别的最新列表在下列地点提供：

www.websense.com/global/en/ProductsServices/MasterDatabase/URLCategories.php

要建议将一个站点添加至主数据库中，单击 Websense Manager 右侧快捷窗格中的**建议新类别**，或前往：

www.websense.com/SupportPortal/SiteLookup.aspx

在登录 MyWebsense 门户之后，您将转至 “站点查找和类别建议”工具。

当您在 Websense Manager 中创建一项**类别筛选器**时，需选择要阻止和允许的类别。

除了储存 URL 类别之外，Websense 主数据库中还包括用于管理非 HTTP Internet 流量的协议组。每个协议组都定义了相似类型的 Internet 协议（如 FTP 或 IRC）和应用程序（如 AOL Instant Messenger 或 BitTorrent）。这些定义每晚都会定期进行验证和更新。

与类别一样，您可以对自定义协议进行定义以用于 Internet 筛选。

主数据库协议的最新列表在下列地点提供：

www.websense.com/global/en/ProductsServices/MasterDatabase/ProtocolCategories.php

当您创建一项**协议筛选器**时，需选择要阻止和允许的协议。

> **注意**
> 必须安装 Network Agent 才能启用基于协议的筛选功能。

某些 Websense 定义的协议可以对向一个外部服务器传送的 Internet 流量加以阻止 – 例如一个特定的即时消息服务器。只有由 Websense 定义并带有动态分配端口号的协议可以作为向外传输流量加以阻止。

新类别和协议

当新类别和协议被添加至主数据库中时，每项都分配到一个默认筛选操作，如**允许**或**阻止**（请参阅*筛选操作*，第 39 页）。

- 所有活动类别和协议筛选器均采用了默认操作（请参阅*筛选器使用*，第 42 页）。编辑活动筛选器，以更改类别或协议的筛选方式。
- 默认操作是根据所讨论的站点或协议是否通常被认为是与业务相关的反馈意见而制定的。

您可以对 Websense 软件进行配置以生成系统警报，当主数据库中添加了新的类别或协议时通知您。请参阅*警报*，第 239 页，以了解更多信息。

特殊类别

主数据库中包含了特殊类别，可帮助您管理特定类型的 Internet 使用情况。所有版本的 Websense 软件均提供有下列类别：

- **特殊事件**类别用于对热门站点进行分类，以帮助您管理 Internet 流量中与事件相关的激变流量。例如，世界杯官方站点通常会出现在“体育”类别中，但是在世界杯决赛阶段期间会被移至“特殊事件”类别之中。

  “特殊活动”类别的更新会在计划下载中添加到主数据库内。当站点被移动至另一类别中或从主数据库中删除之后，会在短时间内被添加至此类别中。
- **效率**类别专注于预防浪费时间的行为。
  - 广告
  - 免费软件与软件下载
  - 即时聊天
  - 在线经纪与交易
  - 上网赚钱
- **带宽**类别专注于节省网络带宽。
  - 网上电台及电视
  - IP 电话
  - 对等文件共享

- 个人网络存储与备份
- 流媒体

Websense Web Security 中包含额外的安全类别：

- **Websense Security Filtering**（亦简称为 **“安全”**）专注于搜寻包含恶意代码并能够绕过病毒探测软件程序的 Internet 站点。此类别的站点将被默认阻止。
  - 机器人网络
  - 键盘记录
  - 恶意网站
  - 网络钓鱼
  - 可能不需要的软件
  - 间谍软件
- **扩展保护**专注于潜在的恶意网站。高风险漏洞和显现的盗用子类别中的站点将被默认阻止。
  - **高风险漏洞**包含隐瞒了其真实性质或身份的站点，或包含暗示潜在恶意目的要素的站点。
  - **显现的盗用**包含发现已知主机和潜在盗用代码的站点。
  - **潜在有害内容**包括可能包含无用内容且具有潜在危害要素的站点。

“扩展保护”组会根据*声誉*对潜在的恶意网站加以筛选。站点声誉均为根据潜在恶意活动的早期征兆而确定。例如，攻击者可能以包含了一般性拼写错误的 URL、或是与合法地址类似的 URL 为目标。这种站点可能被用于在传统筛选器更新并将其标记为恶意站点之前向用户传播恶意软件。

当 Websense 安全研究探测到潜在威胁之后，即会将其添加至拓展保护类别之中，直到 Websense 完全确定该站点的最终归类。

风险级别

相关主题：
- *指定类别的风险级别*，第 256 页
- *演示报告*，第 84 页
- *调查报告*，第 100 页

Websense 主数据库将类别归入不同的**风险级别**。风险级别表明了该组类别中的站点可能存在的漏洞类型或级别。

风险级别主要用于报告之中。“今天”和 “历史”页面中包括按风险级别排序显示的 Internet 活动图，而且您还可以生成按风险级别排列的演示报告或调查报告。

风险级别在创建类别筛选器时也可能十分有用。例如，起初 “基本安全”类别筛选器会阻止 “安全风险”级别中的全部默认类别。当您创建自己的类别筛选器时可以将风险级别分组作为指引来使用，这将有助于确定某个类别应以某种方式允许、阻止或限制。

Websense 软件设有下列 5 个风险级别。按照默认设置，Websense 软件会将下列类别归入各个风险级别之中。

- 一个类别可以出现在多个风险级别中，也可以不分配任何风险级别。
- 主数据库中的分组可以定期更改。

法律责任

成人信息 （包括成人内容、女性内衣与泳装、裸体和性）

带宽 > 对等文件共享

赌博

违法或嫌疑

信息科技 > 黑客入侵与代理回避

暴力冲突与极端主义

种族歧视与仇恨

庸俗

暴力

武器

网络带宽损失

带宽（包括网上电台及电视、IP 电话、对等文件共享、个人网络存储与备份，以及流媒体）

娱乐 > MP3 和音乐下载服务

效率 > 广告和免费软件*与*软件下载

商业使用

商业与经济 （包括金融信息和服务）

教育 > 教学材料*和*参考材料

政府 （包括军事）

信息科技（包括计算机安全、搜索引擎与门户，以及 URL 转换网站）

旅行

交通工具

安全风险

带宽 > 对等文件共享

扩展保护 （包括高风险漏洞、显现的盗用，以及潜在有害内容) [*Websense Web Security*]

信息科技 > 黑客入侵 *与*代理回避

效率 > 免费软件与软件下载

安全（包括机器人网络、键盘记录、恶意网站、网络钓鱼、可能不需要的软件，以及间谍软件）

生产力损失

堕胎 （包括选择优先*与*生命优先）

成人信息 > 性教育

社团组织

带宽 > 网上电台及电视、对等文件共享，以及流媒体

药物 （包括滥用药物、大麻、处方药，以及补充/非管制化合物）

教育 （包括文化机构*和*教育机构）

娱乐 （包括 MP3 和音乐下载服务）

赌博

游戏

政府 > 政治团体

健康

信息科技 > 主机托管

互联网通信 （包括普通电子邮件、企业电子邮件、文本和媒体通信，以及网络聊天室）

求职

新闻与媒体 （包括另类期刊）

效率 （包括免费软件和软件下载、即时聊天、信息布告栏和论坛、在线经纪与交易，以及上网赚钱）

宗教 （包括非传统宗教、秘术与民俗*和*传统宗教）

购物 （包括网上竞拍*和*房地产）

社会组织 （包括职业与工人组织、服务与慈善组织，以及社会与附属组织）

时尚及生活 （包括烟酒、同性恋与双性恋、业余爱好、个人/交友网站、餐饮，以及社交网络和个人站点）

特殊活动

体育运动 （包括狩猎运动与射击俱乐部）

旅行

交通工具

超级管理员可以在**设置 > 风险级别**页面上更改每个类别所分配的风险级别 （请参阅*指定类别的风险级别*，第 256 页）。

安全协议组

除了安全和扩展保护类别之外，Websense Web Security 还设有两项协议，旨在帮助探测和防护通过 Internet 传播的间谍软件和恶意代码或内容。

- **恶意通讯**协议组中包括**机器人网络**协议，旨在对出于恶意而尝试连接 botnet 的 bot 所生成的指令与控制流量进行阻止。
- **恶意通讯 – 仅监视**协议组用于确认可能与恶意软件相关的流量。
  - **通过电子邮件传播的蠕虫病毒**会追踪可能由电子邮件蠕虫袭击所生产的向外传送的 SMTP 流量。
  - **其它恶意通讯**会对怀疑与恶意程序相关的向内和向外传送流量进行追踪。

恶意通讯协议组默认设置为被阻止，并可以在您的协议筛选器中加以配置 （请参阅*编辑协议筛选器*，第 46 页）。恶意通讯 – “仅监视”协议可以进行记录以提供报告，但是不可采用其它的筛选操作。

即时消息附件管理器

即时消息（IM）附件管理器是一项可选功能。如果您订购了此项功能，可以通过 IM 客户端来限制文件共享，包括 AOL/ICQ、 Microsoft （MSN）和 Yahoo。这使您可以在阻止 IM 客户端附件传输的同时还能允许 IM 流量。

即时消息发送文件附件是一个协议组，包含多个 IM 客户端的定义。当启用 IM 附件管理器后，这些协议会出现在 “编辑协议”页面内全部活动协议筛选器的协议列表之中。

内部和外部流量都可以采用 IM 附件筛选。要启用内部流量筛选，应对您的网络部分加以定义来监视**设置 > Network Agent > 全局**页面（请参阅*配置全局设置*，第 290 页）。

筛选操作

类别和协议筛选器会向每个类别或协议分配一项**操作**。这就是 Websense 筛选软件针对客户端的 Internet 请求所采取的应对性操作。适用于类别与协议的操作为：

- **阻止**请求。用户接到阻止页面或阻止消息，而且无法查看站点或使用 Internet 应用程序。
- **允许**请求。用户可以查看站点或使用 Internet 应用程序。
- 在阻止或允许请求之前先评估当前的**带宽**使用情况。当此操作被启用且带宽使用情况达到特定阈值之时，对特定类别或协议的进一步 Internet 请求会被阻止。请参阅*使用 Bandwidth Optimizer 来管理带宽*，第 161 页。

其他操作只能应用于类别之中。

> **注意**
>
> 当个别客户（用户、组、和计算机）由多个 Policy Server 进行管理时，不应使用 “确认”和 “定额”选项。
>
> 与此功能相关的定时信息不会在 Policy Server 之间共享，而受到影响的客户端可能会获得比您计划的更多或更少的 Internet 访问。

- **确认** – 用户进入阻止页面，将被要求确认其是出于业务目的而访问此站点。如果用户单击**继续**，即可以查看站点。

  单击 “继续”开始计时。在配置的时段 （默认为 60 秒）内，用户可以在确认类别中访问其它站点而不会进入另一个阻止页面。当时段终止后，浏览任何其它确认站点将导致进入另一个阻止页面。

  默认时间可以在**设置 > 筛选**页面中进行更改。

- **定额**–用户收到一个阻止页面，将被询问是否要使用定额时间来查看此站点。如果用户单击**使用定额时间**，即可以查看站点。

  单击 “使用定额时间”开始两个计时器：一个定额会话计时器和一个总定额分配计时器。

  - 如果用户在默认**会话**时段 （默认为 10 分钟）内请求额外的定额站点，则他可以访问这些站点而不会收到另一个阻止页面。
  - **总**定额时间将按天进行分配。当其用尽之后，每个客户端必须等至下一天才可访问定额类别中的站点。在**设置 > 筛选**页面中可设置默认的每日定额分配（默认为 60 分钟）。还能以个人为基础对客户端进行每日定额分配。请参阅 *使用定额时间来限制 Internet 访问*，第 40 页，以了解更多信息。
- **阻止关键字**–当您定义了关键字并启用关键字阻止之后，申请 URL 中包含被阻止关键字之站点的用户不许访问该站点。请参阅 *根据关键字筛选*，第 151 页。
- **阻止文件类型**–当启用了文件类型阻止之后，尝试下载类型被阻止之文件的用户会收到一个阻止页面，而且文件不能下载。请参阅 *根据文件类型管理通信*，第 163 页。

使用定额时间来限制 Internet 访问

当用户单击使用定额时间后，在定额会话终止之前可以查看站点的任何定额类别。默认定额会话时间 （通过**设置 > 筛选**页面进行配置）为 10 分钟。

注意

当个别客户端由多个 Policy Server 进行管理时，不应使用定额选项。

与此功能相关的定时信息不会在 Policy Server 之间共享，而受到影响的客户端可能会获得比您计划的更多或更少的 Internet 访问。

定额会话一旦终止后，对定额站点的请求将会收到另一个定额阻止消息。尚未用尽每日定额分配的用户可以开始一次新的定额会话。

一旦定额时间配置之后， Websense 软件将采用优先级列表来决定当用户请求站点的定额类别时如何进行回应。该软件会寻找针对以下方面配置的定额时间：

1. 用户
2. 计算机或网络客户端
3. 用户所属组

   如果用户是多个组的成员， Websense 软件会根据**设置 > 筛选**页面中**使用更强限制性的阻止**设置来分配定额时间 （请参阅 *配置 Websense 筛选设置*，第 49 页）。
4. 默认定额时间

Internet applet 程序，如 Java 或 Flash，对定额时间限制的反应可能与预计情况不同。即使从定额限制网站中访问，在浏览器中运行的 applet 程序仍可以继续运行而免受定额会话时间配置的限制。

这是因为这些 Applet 程序被完全下载至客户端的计算机中并像应用程序一样运行，而无需返回原始主机服务器进行通讯。但是，如果用户单击浏览器的刷新按钮，Websense 软件会探测到与主机服务器的通讯，然后根据适用的定额限制来阻止请求。

密码替代

密码替代使得 Websense 软件可以阻止采用有效密码来访问站点的用户。密码替代可以用于单个客户端（用户、组、计算机或网络）。

当密码替代选项启用后，Websense 会阻止消息，包括一个密码字段。输入有效密码的客户可以在一定时限内访问被阻止的站点。

注意

当个别客户端由多个 Policy Server 进行管理时，不应使用密码替代选项。

与此功能相关的定时信息不会在 Policy Server 之间共享，而受到影响的客户端可能会获得比您计划的更多或更少的 Internet 访问。

密码替代选项可通过**设置 > 筛选**页面启用（请参阅*配置 Websense 筛选设置*，第 49 页）。

通过**策略管理 > 客户端**页面可向特定客户端授予密码替代权限（请参阅*添加客户端*，第 59 页或*更改客户端设置*，第 60 页）。

搜索筛选

Search Filtering 是由某些搜索引擎提供的一项功能，有助于限制不当搜索结果的数目，不将其显示给用户。

通常情况下，Internet 的搜索引擎结果可能包含与搜索标准相匹配的站点的相关缩略图。如果这些缩略图与被阻止站点相关，Websense 软件会阻止用户访问完整的站点，但是不会阻止搜索引擎显示图片。

当您启用 Search Filtering 后，Websense 软件会激活搜索引擎功能，使与被阻止站点相关的缩略图不会在搜索结果中显示。启用 Search Filtering 会同时对本地和远程筛选客户端产生影响。

Websense, Inc.，具有带 Search Filtering 功能的搜索引擎数据库。当数据库中添加或删除了一个搜索引擎时会生成警报（请参阅*警报*，第 239 页）。

Search Filtering 可通过**搜索 > 筛选**页面激活。请参阅*配置 Websense 筛选设置*，第 49 页，以了解更多信息。

筛选器使用

相关主题：

- *筛选类别与协议*，第 34 页
- *Internet 筛选策略*，第 63 页
- *创建类别筛选器*，第 43 页
- *创建协议筛选器*，第 45 页
- *创建受限访问筛选器*，第 143 页

利用 Websense Manager 中的**策略管理 > 筛选器**页面可查看、创建、修改类别和协议筛选器，以及使用其它筛选工具。

筛选器页面分为 3 个主要部分：

- **类别筛选器**会确定要进行阻止和允许的类别。
- **协议筛选器**会确定要进行阻止和允许的非 HTTP 协议。

  必须安装 Network Agent 才能启用基于协议的筛选功能。
- **受限访问筛选器**会确定被允许网站的限制列表（请参阅*限制用户只能访问已定义列表中的 Internet 站点*，第 141 页）。

类别、协议和受限访问筛选器组成了**策略**的构建模块。每项策略均由至少一个类别或受限访问筛选器和一个协议筛选器构成，应用于所选客户端的特定计划之中。

- 要查看或编辑现有类别、协议或受限访问筛选器，请单击筛选器名称。要了解更多信息，请参阅：
  - *编辑类别筛选器*，第 43 页
  - *编辑协议筛选器*，第 46 页
  - *编辑受限访问筛选器*，第 144 页
- 要创建新的类别、协议或受限访问筛选器，请单击**添加**。要了解更多信息，请参阅：
  - *创建类别筛选器*，第 43 页
  - *创建协议筛选器*，第 45 页
  - *创建受限访问筛选器*，第 143 页

要复制一个现有筛选器，请勾选筛选器名称旁边的复选框，然后单击**复制**。副本的名称是由原始筛选器和附带的一串独特数字组合而成，随后会被添加至筛选器列表中。可像编辑其它筛选器一样编辑副本。

如果您已创建了委派管理角色（请参阅*委派管理*，第 197 页），超级管理员可以将他们已创建的筛选器复制给其他角色，供委派管理员使用。

要将筛选器复制给其它角色，应首先勾选筛选器名称旁边的复选框，然后单击**复制到角色**。请参阅*将筛选器和策略复制到角色*，第 145 页，以了解更多信息。

创建类别筛选器

相关主题：

- *筛选器使用*，第 42 页
- *编辑类别筛选器*，第 43 页

利用**策略管理 > 筛选器 > 添加协议筛选器**页面来创建新的类别筛选器。您可以从预定义模板中进行操作，也可复制现有的类别筛选器来用作新筛选器的基础。

1. 输入一个唯一的**筛选器名称**。名称长度必须介于 1 至 50 个字符之间，且不得包含下列符号：

   * < > { } ~ ! $ % & @ # . " | \ & + = ? / ; : ,

   筛选器名称中可以包含空格、连接线和省略符号。
2. 输入筛选器的简短**描述**。此描述会出现在筛选器页面类别筛选器的筛选器名称旁边，应能够解释筛选器的目的。

   筛选器名称的字符限制也适用于描述，但有 2 项例外：描述可包括句点 (.) 和逗号 (,)。
3. 从下拉列表中选择一项，确定要使用模板或是复制现有筛选器。有关了解模板的更多信息，请参阅*类别和协议筛选器模板*，第 48 页。
4. 要查看和编辑新的筛选器，请单击**确定**。筛选器会添加至筛选器页面中的**类别筛选器**列表内。

要自定义筛选器，请单击筛选器名称，然后继续*编辑类别筛选器*。

编辑类别筛选器

相关主题：

- *筛选类别与协议*，第 34 页
- *筛选操作*，第 39 页
- *使用定额时间来限制 Internet 访问*，第 40 页
- *密码替代*，第 41 页
- *筛选器使用*，第 42 页
- *使用类别*，第 147 页

利用**策略管理 > 筛选器 > 编辑类别筛选器**页面可对现有的类别筛选器进行更改。

> **重要**
>
> 当您编辑类别筛选器时，所作的更改会影响执行该筛选器的每一项策略。
>
> 拥有与另一委派管理角色中相同名称的类别筛选器的执行策略不会受到影响。

筛选器名称和描述会出现在页面顶部。

- 单击**重命名**可更改筛选器名称。
- 只需在**描述**字段中输入内容，即可更改筛选器描述。

使用此筛选器的策略旁边的数字显示了所选筛选器目前所使用的策略数量。如果类别筛选器被激活，单击**查看策略**可查看筛选器所执行的策略列表。

页面的底部会显示类别列表和当前对每个类别所采用的操作。

1. 选择**类别**列表中的条目可查看类别信息或更改与所选类别相关的筛选操作。
2. 在更改对类别所应用的操作之前，使用**类别详细信息**部分可查看与该类别相关的任何特殊属性。
   - 要查看分配至类别中的未分类或未经筛选的 URL（如存在），请单击**查看此类别中的自定义 URL**。请参阅*针对特定站点重新定义筛选*，第 153 页。
   - 要查看分配至类别的关键字，请单击**查看此类别中的关键字**。请参阅*根据关键字筛选*，第 151 页。
   - 要查看用来界定类别的自定义 URL 或关键字的正则表达式，请单击**查看此类别中的正则表达式**。
3. 利用类别列表底部的按钮可更改所选类别所应用的操作。要了解可用操作的更多信息，请参阅*筛选操作*，第 39 页。

   委派管理员不能对已由超级管理员锁定之类别的操作进行更改。请参阅*定义所有角色的筛选器限制*，第 221 页，以了解更多信息。
4. 利用类别列表右侧的复选框可对选定类别采用高级筛选操作。
   - 要更改在所选类别筛选中对关键字的使用方式，请勾选或取消**阻止关键字**。*根据关键字筛选*，第 151 页。
   - 要确定用户是否可以从站点的选中类别中访问特定类型的文件，请勾选或取消**阻止文件类型**。请参阅*根据文件类型管理通信*，第 163 页。

     如果您已选择了阻止文件类型，请选择至少一项要阻止的文件类型。
   - 要确定根据特定带宽阈值限制是否能够访问站点的类别，请勾选或取消**使用 Bandwidth Optimizer 阻止**。请参阅*使用 Bandwidth Optimizer 来管理带宽*，第 161 页。

     如果您已选择了按带宽进行阻止，请指明使用的阈值限制。
5. 重复步骤 1 至 3，对其它类别采用的筛选操作进行更改。

6. 在编辑筛选器之后，请单击**确定**，将您的更改存入缓存中并返回筛选器页面。直到您单击**全部保存**之后，更改才会生效实施。

要激活一个新的类别筛选器，请将其添加至一项策略中并将该策略分配给客户端。请参阅 *Internet 筛选策略*，第 63 页。

创建协议筛选器

相关主题：

- *筛选类别与协议*，第 34 页
- *筛选操作*，第 39 页
- *编辑协议筛选器*，第 46 页
- *使用协议*，第 156 页

利用**策略管理 > 筛选器 > 添加协议筛选器**页面来定义新的协议筛选器。您可以从预定义模板中进行操作，也可复制现有的协议筛选器来用作新筛选器的基础。

1. 输入一个唯一的**筛选器名称**。名称长度必须介于 1 至 50 个字符之间，且不得包含下列符号：

   ```
   * < > { } ~ ! $ % & @ # . " | \ & + = ? / ; : ,
   ```

   筛选器名称中可以包含空格、连接线和省略符号。
2. 输入筛选器的简短**描述**。此描述会出现在筛选器页面协议筛选器的筛选器名称旁边，应能够解释筛选器的目的。

   筛选器名称的字符限制也适用于描述，但有 2 项例外：描述可包括句点 (.) 和逗号 (,)。
3. 从下拉列表中选择一项，确定对新的筛选器是使用模板 （请参阅*类别和协议筛选器模板*，第 48 页）还是复制现有筛选器作为基础。
4. 要查看和编辑新的筛选器，请单击**确定**。筛选器会添加至筛选器页面中的**协议筛选器**列表内。

要完成对新筛选器的自定义，请继续*编辑协议筛选器*。

编辑协议筛选器

相关主题：

- *筛选类别与协议*，第 34 页
- *创建协议筛选器*，第 45 页
- *筛选操作*，第 39 页
- *使用协议*，第 156 页
- *使用 Bandwidth Optimizer 来管理带宽*，第 161 页

利用**策略管理 > 筛选器 > 编辑协议筛选器**页面可对现有的协议筛选器进行更改。

重要

在此处所做的更改会影响强制执行该筛选器的所有策略。

拥有与另一委派管理角色中相同名称的协议筛选器的执行策略不会受到影响。

筛选器名称和描述会出现在页面顶部。

- 单击**重命名**可更改筛选器名称。
- 只需在**描述**字段中输入内容，即可更改筛选器描述。

使用此筛选器的策略旁边的数字显示了所选筛选器目前所使用的策略数量。如果协议筛选器被激活，单击**查看策略**可查看筛选器所执行的策略列表。

页面的底部会显示协议列表和当前对每项协议所采用的操作。

要更改协议的筛选和记录方式：

1. 从**协议**列表中选择一项协议。列表右侧会显示对所选协议的高级筛选操作。
2. 利用协议列表底部的**允许**和**阻止**按钮可更改所选协议所应用的操作。

注意

Websense 软件可以阻止基于 TCP 协议的请求，但不能阻止基于 UDP 协议的请求。

某些应用程序可同时采用基于 TCP 和 UDP 的消息。如果应用程序的原始网络申请是通过 TCP 进行的，而随后的数据采用 UDP 发送，则 Websense 软件会阻止初始的 TCP 请求并因而阻止随之而来的 UDP 流量。

UDP 请求可能会被记录为被阻止，即使在被允许时也是如此。

要对所选协议组中的其它协议也采用相同的操作，请单击**应用到组**。

3. 如果您希望将关于所选协议的使用情况信息提供至警报和报告中，请勾选**记录协议数据**复选框。
4. 要将带宽限制加至此协议的使用之中，请单击**使用 Bandwidth Optimizer 阻止**，然后提供要使用的带宽阈值。请参阅*使用 Bandwidth Optimizer 来管理带宽*，第 161 页，以了解更多信息。
5. 在编辑筛选器之后，请单击**确定**，将您的更改存入缓存中并返回筛选器页面。直到您单击**全部保存**之后，更改才会生效实施。

要激活一个新的协议筛选器，请将其添加至一项策略中并将该策略应用至客户端 （请参阅 *Internet 筛选策略*，第 63 页）。

注意

您可以创建策略，开始在特定时间执行协议筛选器的操作。如果用户在筛选器生效之前开始了协议会话，只要在会话持续的情况下，他们即可继续访问协议，即使筛选器阻止该协议。当用户终止会话之后，对该协议的其它请求都将被阻止。

Websense 定义类别与协议筛选器

Websense 软件包含多项样本类别和协议筛选器。您可以直接使用这些筛选器、或对其修改以适合您的筛选需求。如果您不需要预定义筛选器，也可以删除其中的多项。

预定义类别筛选器为：

- 基本
- 基本安全
- 全部阻止
- 默认
- 仅监视
- 全部允许

全部阻止和全部允许类别筛选器未列在筛选器页面中，但可以添加至策略之中。这些筛选器在筛选中有着特殊作用，因此不可删除或编辑。当 Internet 请求被筛选时， Websense 软件会首先检查是否应用了“全部阻止”或“全部允许”筛选器，然后才会进行任何其它筛选检查 （请参阅*筛选站点*，第 69 页）。

预定义协议筛选器为：

- 基本安全
- 默认
- 仅监视
- 全部允许

“全部允许”协议筛选器和与其等效的类别筛选器类似，不列在筛选器页面之中，且不可编辑或删除。在进行筛选时也会优先执行。

对默认类别和协议筛选器可以进行编辑，但是不能删除。在升级环境中，如果“默认”策略中有间隙，则默认筛选器被用于筛选未应用任何策略的请求。

类别和协议筛选器模板

当您创建新的类别或协议筛选器时，您可以通过将现有筛选器复制到筛选器页面，在 “添加筛选器”页面中选择一个现有筛选器为模型，或利用筛选器**模板**来开始操作。

Websense software 中设有 5 个类别筛选器模板：

- **仅监视**和**全部允许**会允许全部类别。
- **全部阻止**会阻止全部类别。
- **基本**会阻止最常阻止的类别并允许其它类别。
- **默认**会对类别采用阻止、允许、继续和定额操作。
- **基本安全**仅会阻止 “安全风险”级别 （请参阅*风险级别*，第 36 页）的默认类别。

Websense software 中还设有 3 个协议筛选器模板：

- **仅监视**和**全部允许**会允许全部协议。
- **基本安全**会阻止 P2P 文件共享和代理回避协议，以及即时消息发送文件附件 （如订购）和恶意通讯 （Websense Web Security）。
- **默认**会阻止即时消息发送协议、P2P 文件共享、代理回避、即时消息发送文件附件 （如订购），以及恶意通讯 （Websense Web Security）。

尽管您可以修改或删除由 Websense 所定义的大部分类别与协议筛选器，却不能编辑或删除模板。与之类似，尽管您可以根据需要来随意创建多项筛选器，却无法创建新模板。

由于模板不可修改，因此可提供回溯参阅由 Websense 定义筛选器采用的原始筛选操作的一致方法。例如，“典型”类别和协议筛选器模板与原始的 “默认”类别和协议筛选器均采用相同的操作。这意味着您随时都可以通过创建采用模板默认内容的筛选器来恢复 Websense 原始筛选配置。

有关利用模板来创建新筛选器的说明，请参阅*创建类别筛选器*，第 43 页或*创建协议筛选器*，第 45 页。

配置 Websense 筛选设置

相关主题：

- *筛选类别与协议*，第 34 页
- *客户端*，第 51 页
- *阻止页面*，第 73 页
- *筛选操作*，第 39 页
- *密码替代*，第 41 页
- *筛选顺序*，第 68 页
- *使用 Bandwidth Optimizer 来管理带宽*，第 161 页
- *根据关键字筛选*，第 151 页

利用**设置 > 筛选**页面可建立基本设置，从而实现各种筛选功能。

在 **Bandwidth Optimizer** 中根据可用的带宽输入所需信息，从而对 Internet 使用情况进行筛选。有关以带宽为基准筛选的更多信息，请参阅 *使用 Bandwidth Optimizer 来管理带宽*，第 161 页。

1. 要指定 **Internet 连接速度**，请进行下列操作之一：
   - 从下拉列表中选择一项标准速度。
   - 在文本字段中输入以千比特/秒为单位的网络速度。
2. 使用**默认网络带宽**字段可输入默认阈值（网络总流量的百分比），供启用网络带宽筛选时加以使用。
3. 使用**每个协议的默认带宽**字段可输入默认阈值，供启用协议带宽筛选时加以使用。

使用**常规筛选**部分来确定当采用多项组策略时如何筛选用户，指定关键字搜索选项，以及设置密码替代、继续和定额会话操作。

1. 要确定采用多项组策略时筛选用户的方法，请勾选或取消**使用最严格的组策略**（请参阅*筛选顺序*，第 68 页）。
   - 选择该选项之后，将采用具有最严格筛选设置的策略。换言之，如果一个适用的组策略阻止了对一个类别的访问而另一项组策略允许该访问，则用户对站点中该类别的请求会被阻止。
   - 未选择该选项时，将采用允许范围最宽的设置。

2. 选择下列**关键字搜索选项**中的一项 （请参阅*根据关键字筛选*，第 151 页）。

仅 CGI	当关键字出现在 CGI 查询字符串（在网址中“?”的后面）中时阻止站点。 示例: **search.yahoo.com/search?p=test** 选中此项时， Websense 软件不会搜索 “?” 之前的关键字。
仅 URL	当关键字出现在 URL 中时阻止站点。如果申请的地址中包含 CGI 查询字符串，Websense 软件会对“?”位置之前进行关键字搜索。
URL 和 CGI	当关键字出现在地址中任何位置时阻止站点。如果出现了一个 CGI 查询字符串，Websense 软件会搜索 “?” 之前和之后的关键字。
禁用关键字阻止	谨慎使用。**禁用关键字阻止**会关闭全部关键字阻止，即使类别筛选器中已选择了**阻止关键字**。

3. 在**密码替代超时**字段中输入用户在选择密码替代之后可以访问站点全部类别的最大秒数（最高为 3600，默认值为 60）（请参阅*密码替代*，第 41 页）。
4. 在**继续超时**字段中输入单击 “继续” 的用户可以访问由确认操作提供的全部类别站点的最大秒数 （最高为 3600，默认值为 60）（请参阅*筛选操作*，第 39 页）。
5. 在**定额会话长度**字段中输入用户可以访问站点中由定额限制之类别 （请参阅*使用定额时间来限制 Internet 访问*，第 40 页）间隔 （最高 60 分钟，默认为 10 分钟）。

   当用户单击 “使用定额时间” 按钮时开始会话。
6. 为全部用户输入**默认每天定额时间** （最高 240 分钟，默认为 60 分钟）。

   要更改单个用户的定额时间，请转至**策略 > 客户端** 页面。

   当您更改定额会话长度和默认每天定额时间后，将计算并显示**默认每天定额会话次数**。

使用**阻止消息**部分可输入您为基于浏览器的阻止消息顶部框架所创建之替代 HTML 阻止页面的 URL 或路径 （请参阅*创建可选阻止消息*，第 79 页）。

- 不同协议可使用各个单独的网页: **FTP**、**HTTP**（包括 **HTTPS**）、和 **Gopher**。
- 将这些字段留空即表明将使用 Websense 软件提供的默认阻止消息或自定义的消息。（请参阅*自定义阻止消息*，第 75 页）。

在 **Search Filtering** 中选择**启用搜索筛选**，可令 Websense 软件激活特定搜索引擎的内置设定，从而在搜索结果中隐藏与被阻止站点相关的缩略图和其它显示内容 （请参阅*搜索筛选*，第 41 页）。

在该部分底部将显示支持此功能的搜索引擎。

当您完成筛选设置的配置之后，请单击**确定**使更改进入缓存。直到您单击**全部保存**之后，更改才会生效实施。

3 客户端

您可以自定义 Websense 软件对特定用户或计算机请求的筛选方式，只需将其添加为 Websense Manager **客户端**。客户端可以是：

- **计算机**：网络中的单台计算机，由 IP 地址加以定义。
- **网络**：一组计算机，由一个 IP 地址范围共同定义。
- **用户**：所支持目录服务中的用户、组、或域帐户。

最初，Websense 会使用**默认**策略（请参阅*默认策略*，第 64 页）以相同的方式对所有客户端进行筛选。当您在 Websense Manager 的 “客户端”页面中添加一个客户端后，就可以向该客户端分配特定的筛选策略。

当采用多项策略时 （如向一个用户分配一项策略并向一台计算机分配另一项策略）， Websense 软件会决定执行哪项策略，如下所述：

1. 向提出请求的**用户**采用所分配的策略。如果该策略在请求时没有计划的筛选器，则使用下一项适用策略。
2. 如果没有适合特定用户的策略，或策略在请求时没有活动的筛选器，将寻找提出请求的**计算机** （首先）或**网络** （其次）所分配到的策略。
3. 如果没有适合特定计算机或网络的策略、或策略在请求时没有活动的筛选器，将寻找用户所属的**组**中所分配到的策略。如果用户属于多个组，则 Websense 软件将考虑适用的全部组策略 （请参阅*筛选顺序*，第 68 页）。
4. 如果没有组策略，则寻找分配至用户**域** (OU) 的策略。
5. 如果未找到适用策略、或策略在请求提出时未执行类别筛选器，则对用户被分配的角色采用**默认**策略。

关于 Websense 软件向客户端采用筛选策略的更多信息，请参阅*筛选站点*，第 69 页。

使用客户端

相关主题：

- *客户端*，第 51 页
- *使用计算机和网络*，第 53 页
- *使用用户和组*，第 54 页
- *添加客户端*，第 59 页
- *更改客户端设置*，第 60 页

使用**策略管理 > 客户端**页面可查看关于现有客户端的信息，添加、编辑、或删除客户端，或是将客户端移动至一个委派管理角色。

如果您是一个委派管理员，则必须在您所管理的客户端列表中添加客户端，才能在“客户端”页面中看到他们。请参阅*添加客户端*，第 59 页，以了解相关说明。

“客户端”分为 3 个组：

- **目录**，其中包括来自您目录服务的用户、组和域（请参阅*使用用户和组*，第 54 页）。
- **网络**，在被筛选的网络中可以由单一策略控制的 IP 地址范围（请参阅*使用计算机和网络*，第 53 页）。
- **计算机**，被筛选网络中通过 IP 地址识别的单台计算机（请参阅*使用计算机和网络*，第 53 页）。

单击客户端类型旁边的加号（+），以查看所选类型中的现有客户端列表。每个客户端列表包括以下内容：

- 客户端名称、IP 地址、或 IP 地址范围。
- 当前分配至用户的**策略**。在分配其它策略之前会采用**默认**策略。（请参阅*Internet 筛选策略*，第 63 页）。
- 客户端是否可以使用**密码替代**选项来查看被阻止的站点（请参阅*密码替代*，第 41 页）。
- 客户端是否有自定义的**定额时间**分配数量（请参阅*使用定额时间来限制 Internet 访问*，第 40 页）。

要查找特定客户端，请浏览树中的适当节点。

要编辑客户端策略、密码替代、定额时间和验证设置，请从列表中选择一个或多个客户端，然后单击**编辑**。请参阅*更改客户端设置*，第 60 页，以了解更多信息。

要添加客户端、或对目前客户端页面中未出现的被管理客户端应用一项策略，请单击**添加**，然后转至*添加客户端*，第 59 页，以了解更多信息。

如果您已创建了委派管理角色（请参阅*委派管理*，第 197 页），超级管理员可以将其客户端移动到其它角色中。首先勾选客户端项旁边的复选框，然后单击**移动到角色**。当一个客户端被移动到被委派管理角色时，该客户端所采用的策略和筛选器都会被复制到该角色中。请参阅*移动客户端到角色*，第 61 页，以了解更多信息。

如果您已将 Websense 软件配置为与基于 LDAP 的目录服务进行通讯，页面顶部的工具栏中会出现**管理自定义 LDAP 组**按钮。[1] 单击该按钮，可添加或编辑基于 LDAP 属性的组（请参阅*使用自定义 LDAP 组*，第 58 页）。

要将一个客户端从 Websense Manager 中删除，请选择该客户端并单击**删除**。

使用计算机和网络

相关主题：

- *使用客户端*，第 52 页
- *使用用户和组*，第 54 页
- *添加客户端*，第 59 页
- *将策略分配给客户端*，第 68 页

在 Websense Manager 中，一台**计算机**是指与一台筛选计算机相关的 IP 地址（例如 10.201.3.1）。**网络**是指与一组筛选计算机相关的 IP 地址范围（例如 10.201.3.2 - 10.201.3.44）。

您可以像对用户、组、或域客户端的操作一样，将策略分配至计算机或网络客户端。

- 例如，向一台不要求用户登录，或者用户可以通过游客账户来访问的**计算机**分配一项策略。
- 向一个**网络**分配一项策略，从而对多台计算机同时采用相同的筛选策略。

当您向一台计算机或一个网络分配一项策略时，无论谁登录到被筛选的计算机上，该策略都会执行，**除非**您已向登录用户分配了策略。该计算机或网络策略的优先权要高于可能应用于该用户的任何**组**策略。

1.

使用用户和组

相关主题：

- *使用客户端*，第 52 页
- *目录服务*，第 54 页
- *使用自定义 LDAP 组*，第 58 页
- *使用计算机和网络*，第 53 页
- *添加客户端*，第 59 页
- *将策略分配给客户端*，第 68 页

为了向您的网络中的单个用户和组应用策略，请将 Websense 软件配置为访问您的目录服务以获取目录对象 （用户、组、域和组织单位）信息。

Websense 软件可以与 Windows NT Directory / Active Directory (Mixed Mode) 通讯，也可以通过轻量级目录访问协议 (LDAP) 来访问 Windows Active Directory、Novell eDirectory，以及 Sun Java System Directory。

注意

当您使用基于 LDAP 的目录服务时，不支持重复的用户名。请确保多个域中不会出现相同的用户名。

此外，如果您使用 Windows Active Directory 或 Sun Java System Directory，不支持密码为空的用户名。请确保所有用户均分配了密码。

Websense User Service 会从目录服务向 Policy Server 和 Filtering Service 传递信息，以供筛选策略使用。

Websense, Inc. 建议您在 Windows 计算机上安装 User Service （尽管也可将其安装在 Linux 计算机上）。通常情况下，该计算机上也安装有 Policy Server。

要配置 Websense 软件与您的目录服务通讯，请参阅 *目录服务*。

目录服务

目录服务是一项储存网络用户和资源相关信息的工具。在能够向 Websense Manager 添加用户客户端（用户、组、域或组织单位）之前，您必须对 Websense 软件进行配置以从您的目录服务中获取信息。

使用**设置 > 目录服务**页面来确认您的网络所使用的目录服务。对于每个 Policy Server，您只可以为一种类型的目录服务配置设置。

首先从目录列表中选择一个目录服务。您所做的选择会决定页面中出现哪些设置。

请参阅相应的部分以了解配置说明：

- *Windows NT Directory / Active Directory (Mixed Mode)*，第 55 页
- *Windows Active Directory (Native Mode)*，第 55 页
- *Novell eDirectory 和 Sun Java System Directory*，第 56 页

Windows NT Directory / Active Directory (Mixed Mode)

如果您的目录服务是 Windows NT Directory 或 Mixed Mode 下的 Active 目录，则无需进一步配置。

在极少数情况下，如果您正采用另一项目录服务，则可能需要在此屏幕上提供额外信息。只有在下列环境中才会出现此情况：

- DC Agent 被用于透明标识（请参阅*DC Agent*，第 178 页）

  和

- User Service 在 Linux 计算机上运行

如果这与您的配置相匹配，请提供 Windows NT Directory / Active Directory (Mixed Mode) 中所列出的管理凭据。如果您的安装未使用此配置，则管理凭据字段将被禁用。

Windows Active Directory (Native Mode)

Windows Active Directory 会在一个或多个*全局编录*中储存用户信息。全局编录让个人和应用程序能够在 Active Directory 域中找到对象（用户、组等等）。

为了使 Websense 软件能够在 Native Mode 下与 Active Directory 通讯，您必须提供关于您的网络中全局编录服务器的信息。

1. 单击全局编录服务器列表旁边的**添加**。“添加全局编录服务器”页面会出现。
2. 使用**服务器 IP 或名称**字段来识别全局编录服务器：
   - 如果您为故障转移配置了多个全局编录服务器，则输入 DNS 域名。
   - 如果您的全局编录服务器未配置故障转移，则请输入要添加之服务器的 IP 地址或主机名（如果您的网络中启用了名称解析）。
3. 输入 Websense 软件应使用来与全局编录通讯的**端口**（默认值为 **3268**）。
4. 此外，您还可以选择输入 Websense 软件在搜索用户信息时应采用的**根上下文**。如果您提供一个值，其必须是您域中有效的上下文。
   - 如果您指定了 3268 或 3269 为通讯端口，则不需要提供根上下文。
   - 如果指定端口为 389 或 636，您必须提供根上下文。
   - 如果根上下文字段留空， Websense 软件会从目录服务的最高级别开始搜索。

注意

避免在多个域中使用相同的用户名。如果 Websense 软件找到一个用户的重复帐户名，该用户将无法被透明识别。

5. 指明 Websense 软件应使用哪个管理帐户来从目录服务中获取用户名和路径信息。此帐户必须能够从目录服务中查询和读取，但无需能够对目录服务进行更改，也不必是域管理员。

   选择**按组件分辨的名称**或**完整的可分辨名称**可指定您希望输入帐户信息的方式。

   - 如果您选择了按组件分辨的名称，则要为管理帐户输入**显示名称**、账户**密码**、**帐户文件夹**，以及 **DNS 域名**。在管理用户名中使用一般名称（cn）格式，而非用户 ID （uid）格式。

     注意

     帐户文件夹字段不支持带有组织单位 (ou) 标签的值（例如 *ou=Finance*）。如果您的管理帐户名中包含一个 ou 标签，请输入管理帐户完整的可分辨名称。

   - 如果您选择了完整的可分辨名称，请在**用户可分辨名称**字段中输入可分辨名称作为单个字符串（例如，*cn=Admin，cn=Users，ou=InfoSystems，dc=company， dc=net*），然后提供该账户的**密码**。

6. 单击**确定**。
7. 对每个全局编录服务器重复上述流程。
8. 单击**高级目录设置**，然后转至*高级目录设置*，第 57 页。

Novell eDirectory 和 Sun Java System Directory

若要从目录服务中检索信息， Websense 软件需要具有管理员权限的用户帐户的可分辨名称、根上下文和密码。

1. 在**服务器 IP** 字段中输入目录服务器计算机的 IP 地址。
2. 输入 Websense 软件将用来与目录通讯的**端口**号。默认值为 389。
3. 如果您的目录对于只读访问需要管理权限，请输入**管理员可分辨名称**和**密码**。
4. 此外，您还可以选择输入 Websense 软件在搜索用户信息时应采用的**根上下文**。例如， *o=domain.com*。

   缩小上下文范围会提高获取用户信息的速度和效率。

   注意

   避免在多个域中使用相同的用户名。如果 Websense 软件找到一个用户的重复帐户名，该用户将无法被透明识别。

5. 单击**高级目录设置**，然后转至*高级目录设置*，第 57 页。

高级目录设置

相关主题：

- *Windows Active Directory (Native Mode)*，第 55 页
- *Novell eDirectory 和 Sun Java System Directory*，第 56 页

这些设置可以用于定义：

- Websense 软件对该目录服务进行搜索，以查找用户、组和域信息的方式
- Websense 软件采用加密连接与目录服务进行通讯
- Websense 软件使用哪些字符集来对 LDAP 信息进行编码

对任何基于 LDAP 的目录服务按需要来配置这些设置。

1. 如果您在目录服务中采用自定义对象级别类型（属性名称），请查看**使用自定义筛选器**。默认筛选器字符串会出现在 “筛选器” 字段中。
2. 编辑现有的筛选器字符串，替代您目录的特定对象级别类型。例如，若您的目录采用了如 **dept** 而非 **ou** （组织单位）的对象级别类型，请在 “域搜索筛选器” 字段中输入新值。

   属性通常是用于搜索目录服务内容的字符串。自定义筛选器会提供在此处所述的功能。

   - **用户搜索筛选器**会决定 User Service 搜索用户的方式。
   - **组搜索筛选器**会决定 User Service 搜索组的方式。
   - **域搜索筛选器**会决定 User Service 搜索域和组织单位的方式。
   - **用户组搜索筛选器**会决定 User Service 将用户与组相关联的方式。
3. 要保证 Websense 软件与您的目录服务之间的通讯安全，请查看**使用 SSL**。
4. 要决定 Websense 软件使用哪些字符集来对 LDAP 信息进行编码，请选择 **UTF-8** 或 **MBCS**。

   MBCS 亦称多字节字符集，通常被用于对如中文、日文及韩文等东亚语言进行编码。
5. 单击**确定**以缓存您的更改。直到您单击**全部保存**之后，更改才会生效实施。

使用自定义 LDAP 组

相关主题：

- *使用用户和组*，第 54 页
- *目录服务*，第 54 页
- *添加或编辑自定义 LDAP 组*，第 58 页

利用**管理自定义 LDAP 组**页面，根据在您的目录服务中所定义的属性来管理自定义组。只有当您将 Websense 软件配置为与基于 LDAP 的目录服务进行通讯时，此选项才可用。

重要

当您将自定义 LDAP 组添加至 Websense Manager 中时，组定义会由活动的 Policy Server 储存，而且不会影响其它 Policy Server 实例。要向多个 Policy Server 添加自定义 LDAP 组，请使用 Websense Manager 登录每个 Policy Server 并输入信息。

如果您添加了自定义 LDAP 组，并且更改了目录服务或更改了目录服务器的位置，则现有的组将变为无效。您必须重新添加组，然后将每一项定义为客户端。

- 要添加组，请单击**添加**（请参阅*添加或编辑自定义 LDAP 组*，第 58 页）。
- 要更改列表中的项，请单击其组名（请参阅*添加或编辑自定义 LDAP 组*）。
- 要删除一个条目，请首先将其选中，然后单击**删除**。

当您完成了对自定义 LDAP 组的更改之后，单击**确定**以缓存更改并返回前一页面。直到您单击**全部保存**之后，更改才会生效实施。

添加或编辑自定义 LDAP 组

使用**添加自定义 LDAP 组**页面可基于您已在目录服务中定义的属性来定义 Websense Manager 中的组。使用**编辑自定义 LDAP 组**页面可更改现有的定义。

重要

如果您添加了自定义 LDAP 组，并且更改了目录服务或更改了目录服务器的位置，则现有的组将变为无效。您必须重新添加组，然后将每一项定义为客户端。

1. 输入或更改**组名**。请使用可以清晰标明 LDAP 组目的的描述性名称。

   组名需区分大小写，且必须具有唯一性。

2. 在您的目录服务中输入或更改定义该组的描述。例如：

   ```
   (WorkStatus=parttime)
   ```

   在本示例中， **WorkStatus** 是一项指明雇佣状态的用户属性，而 **parttime** 则是一个指明用户为兼职员工的值。
3. 单击**确定**返回管理自定义 LDAP 组页面。新的项或修改项会出现在列表中。
4. 添加或编辑其它项，或单击**确定**来缓存更改并返回前一页面。直到您单击**全部保存**之后，更改才会生效实施。

添加客户端

相关主题：

- *使用客户端*，第 52 页
- *使用计算机和网络*，第 53 页
- *使用用户和组*，第 54 页
- *搜索目录服务*，第 60 页
- *更改客户端设置*，第 60 页

使用**策略管理 > 客户端 > 添加客户端**页面可向 Websense Manager 添加用户、组、计算机，以及网络客户端，以便您向其分配策略。

如果您登录了一个委派管理角色，则只能添加出现在您管理的客户端列表中的客户端。在将受管理的客户端添加至客户端页面的流程中，您必须向其分配一项策略。

1. 识别一个或多个客户端：
   - 要添加用户、组或域客户端，请浏览**目录**树以在您的目录服务中查找项。如果您使用的是基于 LDAP 的目录服务，还可以单击**搜索**来启用目录搜索工具 （请参阅*搜索目录服务*，第 60 页）。
   - 要添加一个计算机或网络客户端，请输入 **IP 地址**或 **IP 地址范围**。任意两项网络定义不可重叠，但是网络客户端中可以包含一个被单独识别为计算机客户端的 IP 地址。当出现重叠时，分配至计算机的策略比分配至网络的策略具有优先权。
2. 单击箭头按钮 （>），将每个客户端添加至**选择的客户端**列表中。

   要从 “选择的客户端” 列表中删除项目，请选择客户端并单击**删除**。
3. 选择一个**策略**以分配至 “选择的客户端” 列表中的全部客户端。
4. 在完成后，请单击**确定**以缓存您的更改。直到您单击**全部保存**之后，更改才会生效实施。

客户端会被添加至**策略管理 > 客户端**页面的适当列表中。要更改分配至一个或多个客户端的策略，或配置附加的客户端设置，请选择每个客户端项并单击**编辑**。请参阅*更改客户端设置*，第 60 页，以了解更多信息。

搜索目录服务

如果您已配置 Websense 软件与基于 LDAP 的目录服务通讯，则您可以使用搜索功能来识别用户，将其添加为 Websense Manager 客户端。搜索也可用于将受管理客户端和管理员添加至委派管理角色中。

要搜索目录服务以获取用户、组和组织单位信息：

1. 单击**搜索**。
2. 输入全部或部分用户、组或组织单位**名称**。
3. 使用**类型**列表来指定您想查找的目录项类型 （用户、组、 OU 或全部）。

   在大型目录服务中，选择**所有**可能会导致搜索时间很长。
4. 浏览**搜索上下文**树来指明搜索目录的哪一部分。更准确的上下文会有助于提高搜索速度。
5. 单击**开始**。

   然后就会显示搜索结果列表。
6. 在搜索结果中选择一项或多项，然后单击右侧的箭头 (>) 将每个选择的项添加为客户端或管理员。
7. 单击**新搜索**来输入另一套搜索标准。
8. 单击**浏览**以返回并浏览目录。
9. 完成更改后，请单击**确定**以缓存您的更改。直到您单击**全部保存**之后，更改才会生效实施。

更改客户端设置

使用**策略管理 > 客户端 > 编辑客户端**页面可更改一个或多个客户端的策略和身份验证设置。如果您在单击 “编辑” 之前选择了多个客户端，则在 “编辑客户端” 页面中所作的配置更改将应用到所选的全部客户端中。

1. 选择一个**策略**以应用到所选的客户端。在分配其它策略之前，会对客户端采用默认策略。
2. 要允许用户通过输入密码来替代 Websense 阻止页面，请单击 “密码替代” 下面的**开启**，然后输入并确认密码。

   要删除客户端的密码替代权限，请单击**关闭**。
3. 要为所选客户端分配自定义的**定额时间**，请单击**自定义**，然后输入要分配的定额时间分钟数。

   要还原默认定额设置，请单击**默认**。
4. 单击**确定**以缓存您的更改，然后返回 “客户端” 页面。直到您单击**全部保存**之后，更改才会生效实施。

新客户端设置将出现在**策略管理 > 客户端**页面的客户端列表之中。

移动客户端到角色

超级管理员可以使用**将客户端移动到角色**页面将一个或多个客户端移动到委派管理角色中。移动客户端之后，该客户端会出现在受管理客户端列表和目标角色的客户端页面中。

- 超级管理员角色中客户端所应用的策略及其采用的筛选器会被复制到委派管理角色中。
- 委派管理员可以更改受管理客户端所应用的策略。
- “筛选器锁定”限制不会对超级管理员所管理的客户端造成影响，但是会影响委派管理角色所管理的客户端。
- 如果一个组、域或组织单位被添加至受管理客户端的角色，该角色的委派管理员可以分配策略到组、域或组织单位中的单个用户。
- 如果一个网络 （IP 地址范围）被添加至角色作为受管理客户端，则该角色的委派管理员可以向该网络中的单个计算机分配策略。
- 同一客户端不可移动至多个角色中。

要将所选的客户端移动至委派管理角色：

1. 使用**选择角色**下拉列表来选择一个目标角色。
2. 单击**确定**。

   弹出式对话框会指明所选的客户端已被移动。移动过程可能会需要一段时间。
3. 直到您单击**全部保存**之后，更改才会生效实施。

如果所选角色的委派管理员在移动过程期间以策略访问方式登录，则他们必须先退出 Websense Manager 并重新登录，方可看见“受管理客户端”列表中的新客户端。

4 Internet 筛选策略

相关主题：

- *Internet 使用情况筛选器*，第 33 页
- *客户端*，第 51 页
- *默认策略*，第 64 页
- *使用策略*，第 64 页
- *筛选顺序*，第 68 页

管理用户 Internet 访问的策略。策略由以下内容组成：

- 类别筛选器，用于对网站类别采取操作（允许、阻止）（请参阅*筛选类别与协议*，第 34 页）
- 受限访问筛选器，用于仅允许对有限制网站列表进行访问（请参阅*限制用户只能访问已定义列表中的 Internet 站点*，第 141 页）
- 协议筛选器，用于对 Internet 协议采取操作（请参阅*筛选类别与协议*，第 34 页）
- 用于确定何时强制执行每个类别或受限访问筛选器和协议筛选器的计划

新 Websense 软件安装包括 3 种预定义策略：

- **默认**将筛选未由其他策略管理的所有客户端的 Internet 访问。输入订购密钥后，Websense 软件就会开始强制执行此策略（请参阅*默认策略*，第 64 页）。
- **不受限**提供不受限制的 Internet 访问。默认情况下此策略不会应用到任何客户端上。
- **示例 – 标准用户**显示如何在一个策略中应用多个类别和协议筛选器，以便在不同时间提供不同程度的筛选限制。新用户快速入门教程中将使用本策略来演示编辑一项策略并将其应用于客户端的过程。

照原样使用这些策略，编辑这些策略使其适合您的机构，或创建自己的策略。

默认策略

相关主题：

- *Internet 筛选策略*，第 63 页
- *使用策略*，第 64 页
- *筛选顺序*，第 68 页

安装 Websense 软件时，一旦您输入订购密钥，**默认**策略就会开始监视 Internet 使用情况。起初，默认策略将允许所有请求。

注意

当您从较早的 Websense 软件版本升级时，会保存现有的策略设置。升级完毕后，请检查您的策略以确保其仍然正确无误。

当您创建并应用自己的筛选策略后，默认策略会继续充当安全网，对任何没有被其它策略管理的客户端进行 Internet 访问筛选。

在新的安装中，默认策略必须一周七天，一天 24 小时提供 Internet 筛选管理（强制执行类别访问筛选器或受限访问筛选器和协议筛选器的筛选器组合，如适用）。

重要

从之前 Websense 软件版本升级的软件可能会采用并未覆盖所有时间段的默认策略。您不需要更改自己的默认策略。但是，如果您在今后编辑策略，Websense 软件只有当您覆盖所有时间段后才会允许您保存更改。

根据需要编辑默认策略，以符合您机构的需求。默认策略不能删除。

使用策略

相关主题：

- *Internet 筛选策略*，第 63 页
- *创建策略*
- *编辑策略*
- *Internet 使用情况筛选器*
- *改善筛选策略*

使用**策略管理 > 策略**页面可查看当前策略信息。本页也可作为启动点来添加、编辑和删除策略，复制策略给委派管理角色（仅超级管理员），以及打印有关您策略配置的详细信息。

策略页包括现有策略列表。列表包括每项策略的名称和描述、用户数量、网络，以及策略被分配到的计算机客户端。

- 要添加策略，请单击**添加**，然后查看*创建策略*，第 65 页，以了解更多信息。
- 要编辑策略，请单击列表中的策略名称，然后查看*编辑策略*，第 66 页，以了解更多信息。
- 要查看该策略被用于筛选哪些客户端，请单击“用户”、“网络”或“计算机”列中的数字。客户端信息将出现在弹出式对话框中。

要打印您的全部策略及其组件的列表（包括筛选器、自定义类别和协议、关键词、自定义 URL，以及正则表达式），请单击**将策略打印到文件**。此功能会创建一个 Microsoft Excel 格式的详细策略信息电子表格。它旨在为具有监管权限的人力资源专员、经理和其他人提供一种查看筛选策略信息的便捷方式。

如果您已创建了委派管理角色（请参阅*委派管理*，第 197 页），则超级管理员可以将他们创建的策略复制给其他角色，供委派管理员使用。还会复制由策略强制执行的筛选器。

注意

由于委派管理员由筛选器锁定进行管理，因此“全部允许”筛选器和强制执行它们的策略将无法复制到角色。

要将策略复制给其他角色，应首先勾选策略名称旁边的复选框，然后单击**复制到角色**。请参阅*将筛选器和策略复制到角色*，第 145 页，以了解更多信息。

创建策略

相关主题：

- *Internet 筛选策略*，第 63 页
- *使用策略*，第 64 页
- *编辑策略*，第 66 页
- *筛选器使用*，第 42 页
- *限制用户只能访问已定义列表中的 Internet 站点*，第 141 页

使用**策略管理 > 策略 > 添加策略**页面可创建新的自定义策略。

1. 输入一个唯一的**策略名称**。策略名称长度必须介于 1 到 50 个字符之间，且不得包括下列字符：

   ```
   * < > { } ~ ! $ % & @ # . " | \ & + = ? / ; : ,
   ```

   策略名称可以包括空格、连接线和省略符号。

2. 输入策略**描述**。该描述应该清楚并且详细，从而有助于长期的策略管理。

   策略名称的字符限制也适用于描述，但有 2 项例外：描述可包括句点 (.) 和逗号 (,)。

3. 要使用现有策略作为新策略的基础，请勾选**基于现有策略**复选框，然后从下拉列表中选择一个策略。

   要从空白策略开始，则不用勾选复选框。

4. 单击**确定**以缓存您的更改，然后转至 “编辑策略” 页面。

   使用 “编辑策略” 页来完成新策略定义。请参阅*编辑策略*，第 66 页。

编辑策略

相关主题：

- *Internet 筛选策略*，第 63 页
- *使用策略*，第 64 页
- *创建策略*，第 65 页
- *筛选器使用*，第 42 页
- *限制用户只能访问已定义列表中的 Internet 站点*，第 141 页

使用**策略管理 > 策略 > 编辑策略**页面可现有策略进行更改，或者完成定义新策略。

使用页面顶部来编辑策略名称和描述：

- 单击**重命名**可更改策略名称。
- 只需在**描述**字段中输入内容，即可更改筛选器描述。

在策略描述下方，**客户端**字段会列出本策略目前会筛选的各类客户端 （用户、计算机和网络）的数量。要了解哪些客户端受到策略管理，请单击与相应客户端类型相对应的链接。

要将此策略分配给其它客户端，请单击页面顶部工具栏中的**应用到客户端**，然后查看*将策略分配给客户端*，第 68 页。

使用**策略定义**区域可定义此策略在不同时间应用的筛选器：

1. 要向计划添加时间块，请单击**添加**。
2. 使用计划表中的**开始**和**结束**列可定义此时间块覆盖的时间段。

   要为跨子夜 （例如下午 5 点到早 8 点）的一段时间定义筛选，请向计划添加两个时间块：其中一个时间块覆盖从开始时间到子夜的时间段，而另一个时间块则覆盖从子夜到结束时间的时间段。

   示例 – 标准用户策略 （包括在 Websense 软件中）将演示如何定义跨越子夜的筛选时间段。

3. 使用**天数**列可定义该时间块中包括一周中的哪几天。要从列表中选择天数，请在列的右边部分单击向下箭头。选择完天数后，单击向上箭头。
4. 使用**类别/受限访问筛选器**列可选择一个在此时间块内强制执行的筛选器。

   要添加一个在此策略中强制执行的新筛选器，请选择**创建类别筛选器**或**创建受限访问筛选器**。请参阅*创建类别筛选器*，第 43 页或*创建受限访问筛选器*，第 143 页，以了解相关说明。
5. 使用**协议筛选器**列可选择一个在此时间块内强制执行的协议筛选器。

   要添加一个在此策略中强制执行的新筛选器，请选择**创建协议筛选器**。请参阅*创建协议筛选器*，第 45 页，以了解相关说明。
6. 重复步骤 1 到 5，在计划中添加其它时间块。

当选择计划内的任何时间块后，“编辑策略”页面的底部将显示该时间块内强制执行的筛选器。每个筛选器列表包括以下内容：

- 筛选器类型 （类别筛选器、受限访问筛选器或协议筛选器）
- 筛选器名称和描述
- 筛选器内容 （类别或协议，以及采用的操作，或允许的站点列表）
- 强制执行所选筛选器的策略数量
- 可用于编辑筛选器的按钮

当您在本页面中编辑筛选器时，所作的更改会影响强制执行该筛选器的每一项策略。在编辑由多项策略强制执行的筛选器前，请单击**使用此筛选器的策略数**链接，以查看具体有哪些策略会受到影响。

根据筛选器类型，出现在筛选器列表底部的按钮：

筛选器类型	按钮
类别筛选器	• 使用**允许**、**阻止**、**确定**或**定额**按钮可更改应用于所选类别的操作 （请参阅*筛选操作*，第 39 页）。 • 要更改应用于一个父类别及其所有子类别的操作，请首先更改应用于父类别的操作，然后单击**应用到子类别**。 • 要启用关键字阻止、文件类型阻止或基于带宽的阻止，请单击**高级**。
受限访问筛选器	• 使用**添加站点**和**添加表达式**按钮可将允许的 URL、IP 地址或正则表达式添加至筛选器 （请参阅*限制用户只能访问已定义列表中的 Internet 站点*，第 141 页）。 • 要从筛选器中删除某个站点，请勾选 URL、IP 地址或表达式旁边的复选框，然后单击**删除**。
协议筛选器	• 使用**允许**或**阻止**按钮可更改应用于所选协议的操作（请参阅*筛选操作*，第 39 页）。 • 要更改应用于协议组中所有协议的操作，请更改应用于组内任何协议的操作，然后单击**应用到组**。 • 要记录所选协议的数据，或者要启用基于带宽的阻止，请单击**高级**。

完成编辑策略后，请单击**确定**以缓存您的更改。直到您单击**全部保存**之后，更改才会生效实施。

将策略分配给客户端

相关主题：

- *Internet 筛选策略*，第 63 页
- *创建策略*，第 65 页
- *编辑策略*，第 66 页
- *客户端*，第 51 页
- *添加客户端*，第 59 页

使用**策略 > 编辑策略 > 将策略应用到客户端**页面将所选策略分配给客户端。

客户端列表会显示所有可用的用户、计算机和网络客户端，以及当前分配到每个客户端的策略。

勾选将要由选定策略筛选的每个客户端旁边的复选框，然后单击**确定**以返回到“编辑策略”页。再次单击**确定**以缓存您的更改。

单击**全部保存**，提示 Websense 软件开始使用新策略来筛选选定客户端发出的请求。

筛选顺序

Websense 软件使用多个筛选器，并按特定顺序应用，以确定是允许、阻止还是限制请求的 Internet 数据。

对于收到的每个请求， Websense 软件会：

1. 验证订购一致性，确保订购为当前订购且订购客户端的数量没有超出。
2. 确定应用的策略，按以下顺序搜索：
   a. 分配到**用户**的策略。
   b. 分配到所用设备 **IP 地址**（计算机或网络）的策略。
   c. 分配到用户所属**组**的策略。
   d. 分配到用户**域**的策略。
   e. **默认**策略。

   将使用找到的第一个适用策略。
3. 根据策略的限制来筛选请求。

在某些情况下，用户会属于多个组或域，这时没有适用的用户、计算机或网络策略。在这种情况下， Websense 软件会检查分配到每个用户组的策略。

- 如果所有组拥有相同的策略， Websense 软件会根据该策略来筛选请求。
- 如果其中一个组拥有不同的策略，则 Websense 软件会根据**设置 > 筛选**页面上的**使用更强限制性的阻止**选择来筛选请求。

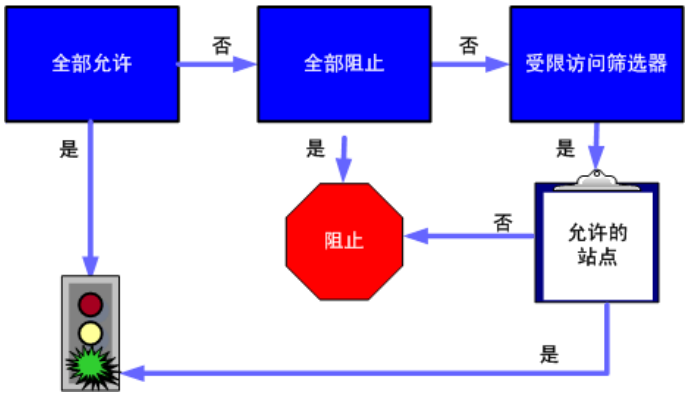
  如果勾选了**使用更强限制性的阻止**，且任何适用的策略阻止了对所请求类别的访问，则 Websense 软件会阻止该站点。

  如果未勾选此选项，且任何适用的策略允许对所请求类别的访问，则 Websense 软件会允许该站点。

如果其中一个适用的策略强制执行受限访问筛选器，则**使用更强限制性的阻止**选项可能会产生不同于预期的效果。请参阅*受限访问筛选器和筛选优先权*，第 142 页。

筛选站点

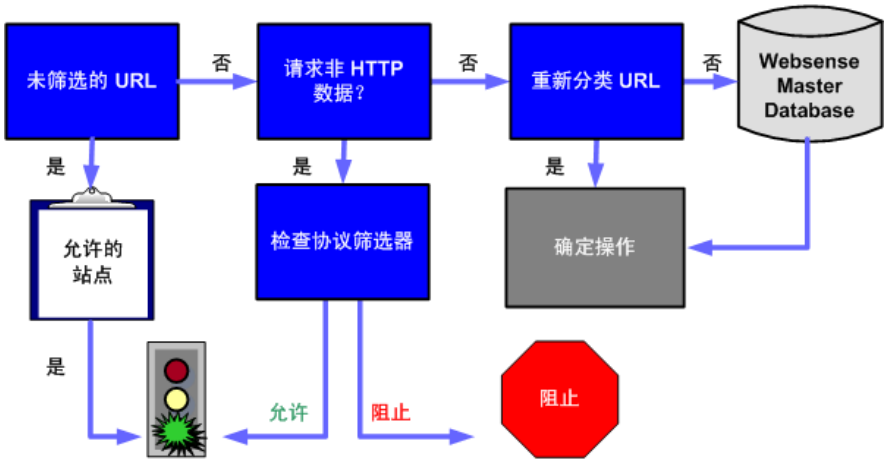
Websense 软件会评估如下策略限制，以确定应该允许还是阻止请求的站点。



1. 确定策略在当前日和当前时间强制执行哪个**类别筛选器**或**受限访问筛选器**。
   - 如果活动的类别筛选器为**全部允许**，则允许该站点。
   - 如果活动的类别筛选器为**全部阻止**，则阻止该站点。
   - 如果筛选器为**受限访问筛选器**，请检查筛选器是否包含 URL 或 IP 地址。如果包含，则允许该站点。如果不包含，则阻止该站点。

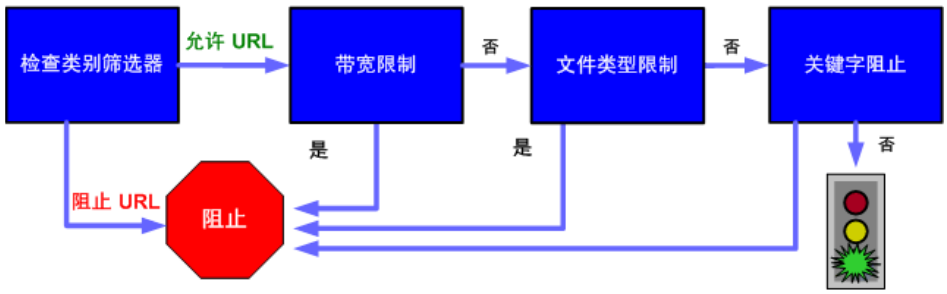
- 如应用了任何其它类别筛选器，请继续步骤 2。

> **注意**
>
> Websense 软件会筛选通过 Internet 搜索引擎访问的 URL，就像筛选任何其它 URL 一样。采用这种方式存储的 URL 会根据为其 URL 类别激活的策略来进行筛选。已缓存 URL 的日志记录会显示整个已缓存的 URL，包括任何搜索引擎参数。

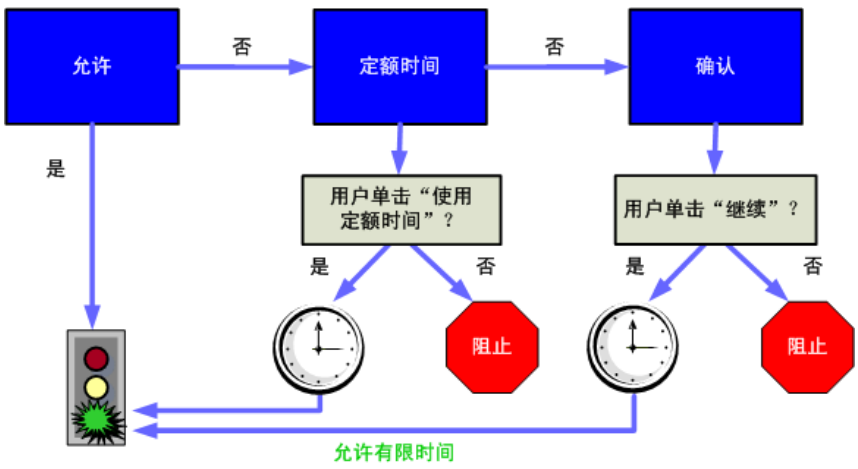


2. 尝试将站点与**未筛选的 URL** 列表中的条目相匹配。
   - 如果 URL 在列表中出现，则允许该站点。
   - 如果 URL 未在列表中出现，则继续步骤 3。
3. 勾选活动的**协议筛选器**，并确定非 HTTP 协议是否与此请求相关联。
   - 如果有关联，应将协议筛选设置应用于可以传送的数据。
   - 如果没有关联，应继续步骤 4。
4. 尝试将站点与**重新分类 URL** 列表中的条目相匹配。
   - 如果进行了匹配，应识别站点的类别，然后转到步骤 6。
   - 如果没有进行匹配，则继续步骤 5。
5. 尝试将站点与**主数据库**中的条目相匹配。
   - 如果 URL 出现在主数据库中，应识别站点的类别，然后继续步骤 6。

- 如果没有进行匹配，应将站点分类为其它/未分类，然后继续步骤 6。



6. 检查活动的类别筛选器，然后识别应用于包含所请求站点之类别的操作。
   - 如果操作为**阻止**，则阻止站点。
   - 如应用了任何其它操作，请继续步骤 7。
7. 检查活动类别筛选器中的 **Bandwidth Optimizer** 设置（请参阅 *使用 Bandwidth Optimizer 来管理带宽*，第 161 页）。
   - 如果当前带宽使用超出任何配置的限制，则阻止该站点。
   - 如果当前带宽使用没有超出特定限制，或者没有应用基于带宽的操作，则继续步骤 8。
8. 检查应用于该活动类别的**文件类型**限制（请参阅 *根据文件类型管理通信*，第 163 页）。
   - 如果站点包含其扩展名在阻止范围内的文件，则会阻止对这些文件的访问。如果站点本身由被阻止的文件类型组成，则阻止对站点的访问。
   - 如果站点不包含扩展名被阻止的文件，则转至步骤 9。
9. 如果启用了关键字阻止，请检查 URL 和 CGI 路径中是否有被阻止的**关键字**（请参阅 *根据关键字筛选*，第 151 页）。
   - 如果找到了被阻止的关键字，则阻止该站点。
   - 如果没有找到被阻止的关键字，请继续步骤 10。



10. 根据应用于该类别的操作来处理站点。
    - **允许**：允许站点。
    - **按定额限制**：显示阻止消息，选项包括使用定额时间查看站点或者返回上一页。
    - **确认**：显示阻止消息，选项包括查看用于工作目的的站点。

Websense 软件会继续操作，直到请求的站点被阻止或被明确允许。此时，Websense 软件不会尝试任何进一步的筛选。例如，如果某个请求的站点属于被阻止的类别并包含某个被阻止的关键字， Websense 软件就会在类别级别即阻止该站点，而无需检查关键字筛选。Log Server 随后会将记录，该请求被阻止是因为其类别，而非因关键字。

注意

具有密码替代权限的用户不管站点因任何原因被阻止，都可以访问 Internet 站点。

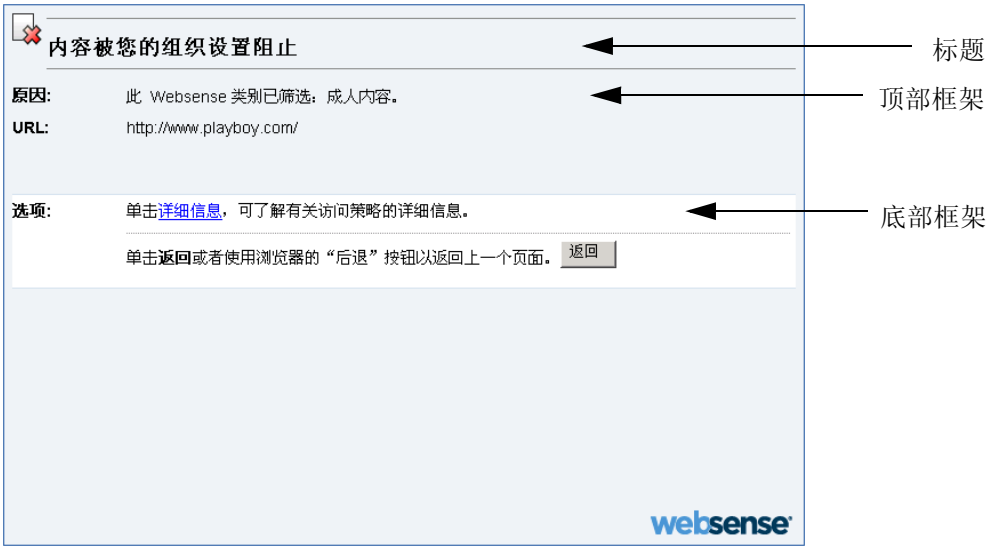
5 阻止页面

相关主题：

- *协议阻止消息*，第 74 页
- *使用阻止页面*，第 75 页
- *创建可选阻止消息*，第 79 页
- *在其他计算机上使用可选阻止页面*，第 79 页

当 Websense 软件阻止一个网站时，将会在客户端浏览器中显示阻止页面。如果该网站由于属于“安全风险”级别中的类型而被阻止（请参阅*风险级别*，第 36 页），则会显示特殊版本的阻止页面。

默认情况下，阻止页面由 3 个主要部分组成。



- **标题**将显示站点被阻止的原因。
- **顶部框架**包含相关阻止信息，将显示被请求的 URL 以及该 URL 被阻止的原因。
- **底部框架**将显示用户可用的选项，如返回前页，或是单击“继续”或“使用定额时间”按钮以查看站点。

阻止页面以 HTML 文件为基础进行构建。您的 Websense 软件中已包含默认阻止页面文件。您可使用这些默认文件或是创建您自己的自定义版本。

- 自定义默认文件以更改阻止消息（请参阅*使用阻止页面*，第 75 页）。
- 配置 Websense 软件以使用远程 Web 服务器上的阻止消息（默认或自定义）（请参阅*在其他计算机上使用可选阻止页面*，第 79 页）。

协议阻止消息

相关主题：

- *使用阻止页面*，第 75 页
- *创建可选阻止消息*，第 79 页
- *在其他计算机上使用可选阻止页面*，第 79 页

当用户或应用程序请求一个被阻止的非 HTTP 协议时，Websense 软件通常会显示一个协议阻止消息。

然而，如果用户在浏览器内请求一个被阻止的 FTP、HTTPS、或 Gopher 站点，且该请求需通过代理，则浏览器内将显示一个基于 HTML 的阻止页面。

如果应用程序请求被阻止的协议，则用户可能也会收到来自应用程序的错误消息，表明该应用程序无法运行。应用程序错误消息并非由 Websense 软件生成。

在 Windows 计算机上显示协议阻止消息可能需要一定的系统配置：

- 要在运行 Windows NT、XP 或 200x 的计算机上显示协议阻止消息，必须启动 Windows Messenger 服务。默认情况下，该服务处于禁用状态。您可查看“Windows 服务”对话框以确定在指定的计算机上该服务是否正在运行（请参阅*Windows 服务对话框*，第 334 页）。
- 要在运行 Windows 98 的计算机上显示协议阻止消息，必须启动 Windows 目录下的 **winpopup.exe**。您可通过命令提示窗口运行该应用程序，或是将其复制到“启动”文件夹中将其配置为自动启动。

协议阻止消息在 Linux 计算机中无法显示；而 HTML 阻止页面在任何操作系统中均可显示。

如果启动了协议筛选功能，则无论客户端计算机是否被配置为可显示协议阻止消息，Websense 软件都将对协议请求进行筛选。

使用阻止页面

相关主题：
- *协议阻止消息*，第 74 页
- *自定义阻止消息*，第 75 页
- *创建可选阻止消息*，第 79 页
- *在其他计算机上使用可选阻止页面*，第 79 页

用于创建 Websense 阻止页面的文件存储于 **Websense\BlockPages\en\Default** 目录中。

- **master.html** 可为阻止页面构建消息框架，并使用以下文件之一在底部框架中显示适用选项。

文件名	内容
blockFrame.html	被阻止类别中站点的文本和按钮（“返回”选项）。
continueFrame.html	适用于**确认**操作类别中站点的文本和按钮。
quotaFrame.html	适用于**定额**操作类别中站点的文本和按钮。
moreInfo.html	用户单击阻止页面上的**更多信息**链接时出现的页面上所包含的内容。

- **block.html** 包含阻止消息的顶部框架文本，将说明访问被限制、列出被请求的站点，并描述站点被限制的原因。

自定义阻止消息

相关主题：
- *更改消息框架的尺寸*，第 76 页
- *更改阻止页面上显示的徽标*，第 77 页
- *使用阻止页面内容变量*，第 77 页
- *还原至默认阻止页面*，第 78 页

您可复制默认阻止页面文件，然后利用该副本自定义用户接收到的阻止页面的顶部框架。

- 添加与贵组织的互联网使用策略有关的信息。
- 就互联网使用策略提供人力资源部门或 Websense 管理员的联系方式。

1. 转至 Websense 阻止页面目录：

   `< 安装路径 >\BlockPages\en\Default`

2. 将阻止页面文件复制到自定义阻止页面目录：

   `< 安装路径 >\BlockPages\en\Custom`

   注意

   请勿修改 **BlockPages\en\Default** 目录中的原始阻止消息文件。您可将它们复制到 **BlockPages\en\Custom** 目录中，然后修改副本文件。

3. 使用 Notepad 或 vi 等文本编辑器打开文件。

   警告

   使用无格式文本编辑器编辑阻止消息文件。有些 HTML 编辑器会修改 HTML 代码，这样可能会损坏文件并导致在显示阻止消息时出现问题。

4. 修改文本。文件中包含有指导您进行更改的注释。

   请勿修改令牌（由 $* 和 *$ 符号圈起）或修改 HTML 代码的结构。这些可使 Websense 软件在阻止消息中显示特定信息。

5. 保存文件。
6. 重新启动 Filtering Service （请参阅*停止和启动 Websense 服务*，第 238 页，以获取说明）。

更改消息框架的尺寸

根据您希望在阻止消息中提供的信息不同，阻止消息的默认宽度和顶部框架的高度也可能不同。要在 **master.html** 文件中更改这些尺寸参数：

1. 请将 **Websense\BlockPages\en\Default** 目录中的 **master.html** 复制到 **Websense\BlockPages\en\Custom** 目录中。
2. 然后使用 Notepad 或 vi 等文本编辑器 （不是 HTML 编辑器）打开文件。
3. 要更改消息框架的宽度，请编辑以下行：

   ```
   <div style="border: 1px solid #285EA6;width: 600px...">
   ```

   然后按要求更改 **width** 参数的值。

4. 要将消息的顶部框架改成滚动模式以显示其他信息，请编辑以下行：

   ```
   <iframe src="$*WS_BLOCKMESSAGE_PAGE*$*WS_SESSIONID*$" ...
   scrolling="no" style="width:100%; height: 6em;">
   ```

   并将 **scrolling** 参数的值更改为 **auto**，从而在消息文本超出框架高度时显示滚动条。

   您也可更改 **height** 参数的值以更改框架高度。

5. 保存并关闭文件。
6. 重新启动 Filtering Service 以执行更改（请参阅*停止和启动 Websense 服务*，第 238 页）。

更改阻止页面上显示的徽标

master.html 文件中也包括用于在阻止页面上显示 Websense 徽标的 HTML 代码。要改为显示您的组织的徽标：

1. 如果还未复制 **Websense\BlockPages\en\Default** 目录中的阻止页面文件，请将其复制到 **Websense\BlockPages\en\Custom** 目录中。
2. 接着将包含您的组织徽标的图像文件复制到相同位置。
3. 使用 Notepad 或 vi 等文本编辑器（不是 HTML 编辑器）打开 **master.html**，并编辑以下行，从而将 Websense 徽标替换成您的组织的徽标。

   ```
   <img title="Websense" src="/en/Custom/wslogo_block_page.png"
   ...>
   ```

   - 将 **wslogo_block_page.png** 替换成包含组织徽标的图像文件的名称。
   - 替换 **title** 参数的值以反映您的组织的名称。
4. 保存并关闭文件。
5. 重新启动 Filtering Service 以执行更改（请参阅*停止和启动 Websense 服务*，第 238 页）。

使用阻止页面内容变量

内容变量可控制 HTML 阻止页面上显示的信息。以下变量被包含在默认阻止消息代码中。

变量名称	显示的内容
WS_DATE	当前日期
WS_USERNAME	当前用户名（不含域名）
WS_USERDOMAIN	当前用户的域名
WS_IPADDR	请求源计算机的 IP 地址
WS_WORKSTATION	被阻止计算机的名称（若无名称，则显示 IP 地址）

要使用变量，请在适当的 HTML 标签中的 $* *$ 符号之间插入变量名称。

```
<p id="UserName">$*WS_USERNAME*$</p>
```

在这里， *WS_USERNAME* 即指变量。

阻止消息代码还包括如下所述的其他变量。其中一些变量在您构建自己的自定义阻止消息时将十分有用。但是当您在 Websense 定义的阻止消息文件中查看这些变量时，请**勿**进行修改。因为 Filtering Service 会在处理被阻止的请求时使用这些变量，因此它们必须保留不作修改。

变量名称	目的
WS_URL	显示被请求的 URL
WS_BLOCKREASON	显示站点被阻止的原因（例如，应用了哪个筛选操作）
WS_ISSECURITY	指明被请求的站点是否属于安全风险级别中的任何默认类别。如果属于，则将显示安全阻止页面。
WS_PWOVERRIDECGIDATA	包含阻止页面的 HTML 代码中带**密码替代**按钮使用信息的输入字段。
WS_QUOTA_CGIDATA	包含阻止页面的 HTML 代码中带**使用定额时间**按钮使用信息的输入字段。
WS_PASSWORDOVERRID_BEGIN、WS_PASSWORDOVERRID_END	涉及激活密码替代功能方面的信息
WS_MOREINFO	显示有关请求站点被阻止原因的详细信息（单击**更多信息**链接后显示）
WS_POLICYINFO	指明请求客户端受何种策略管理
WS_MOREINFOCGIDATA	向 Filtering Service 发送关于**更多信息**链接使用情况的数据
WS_QUOTATIME	显示请求客户端剩余的定额时间长短
WS_QUOTAINTERVALTIME	显示为请求客户端配置的定额会话长度
WS_QUOTABUTTONSTATE	指明进行特殊请求时，**使用定额时间**按钮处于启动还是禁用状态
WS_SESSIONID	用作与请求相关联的内部标识符
WS_TOPFRAMESIZE	在配置了自定义阻止服务器的情况下，指明由该服务器发送的阻止页面顶部的尺寸（以百分数表示）
WS_BLOCKMESSAGE_PAGE	指明用于阻止页面顶部框架的源
WS_CATEGORY	显示被阻止的 URL 的类别
WS_CATEGORYID	被请求的 URL 类别的唯一标识符

还原至默认阻止页面

如果用户在您执行自定义阻止消息后遇到错误，您可以按以下步骤恢复默认阻止消息：

1. 删除 **Websense\BlockPages\en\Custom** 目录中的所有文件。默认情况下，Websense 软件将返回使用 Default 目录中的文件。
2. 重新启动 Filtering Service（请参阅 *停止和启动 Websense 服务*，第 238 页）。

创建可选阻止消息

相关主题：

- *使用阻止页面*，第 75 页
- *自定义阻止消息*，第 75 页

您可创建您自己的 HTML 文件，以提供将显示在阻止页面顶部框架中的文本。您可使用现有的 HTML 文件、完全重新创建可选文件，或复制 **block.html** 以作为模板使用。

- 为 3 个不同协议创建各自不同的阻止消息：HTTP、 FTP 和 Gopher。
- 将文件放置到 Websense 计算机或是您的内部 Web 服务器上（请参阅 *在其他计算机上使用可选阻止页面*，第 79 页）。

创建可选阻止消息文件后，您必须将 Websense 软件配置为显示新消息（请参阅 *配置 Websense 筛选设置*，第 49 页）。进行配置时，您可为每个可配置协议指定各自使用的消息。

在其他计算机上使用可选阻止页面

相关主题：

- *使用阻止页面*，第 75 页
- *自定义阻止消息*，第 75 页
- *创建可选阻止消息*，第 79 页

您也可以不使用 Websense 阻止页面而仅对顶部框架消息进行自定义，您可以创建您自己的 HTML 阻止页面并将其放置到内部 Web 服务器上。

注意

您也可以在外部 Web 服务器上存储阻止页面。但是，如果该服务器上放置了主数据库中列出的站点，而该站点属于被阻止类别，则阻止页面本身就会被阻止。

有些组织会使用可选、远程的阻止页面以隐藏 Websense 服务器计算机的身份。

远程阻止页面可以是任何 HTML 文件，且无需遵从默认 Websense 阻止页面的格式。但是，使用这种方法来创建阻止页面时，您将无法使用“继续”、“使用定额时间”和 “密码替代”等在采用 Websense 定义的阻止页面 （默认或自定义均可）时可使用的功能。

当文件被放置到适当位置后，编辑 **eimserver.ini** 文件以指向新的阻止页面。

1. 依次停止 Websense Filtering Service 和 Policy Server 服务（请参阅*停止和启动 Websense 服务*，第 238 页）。
2. 在 Filtering Service 计算机上，转至 Websense **bin** 目录 （默认情况下，路径为 \Program Files\Websense\bin 或 /opt/websense/bin）。
3. 创建 **eimserver.ini** 文件的备份副本并将其存储到其他目录中。
4. 在文本编辑器中打开 **eimserver.ini** 文件，然后查找 **[WebsenseServer]** 部分（位于文件顶部）。
5. 按以下格式输入放置阻止页面的服务器的主机名称或 IP 地址：

   ```
   UserDefinedBlockPage=http://< 主机名称或 IP 地址 >
   ```

   必须输入 URL 的协议部分 (http://)。
6. 保存文件并关闭文本编辑器。
7. 依次重新启动 Websense Policy Server 和 Filtering Service。

这些服务启动后，用户将收到放置在可选计算机上的阻止页面。

6 使用报告以评估筛选策略

相关主题：

- *报告概述*，第 82 页
- *演示报告*，第 84 页
- *调查报告*，第 100 页
- *访问自我报告*，第 121 页

Websense Manager 可为您提供一些用于评估筛选策略有效性的报告工具。（Websense Manager 和 Websense 报告组件必须安装在 Windows 服务器上。）

- 打开 Websense Manager 时首先将出现**今天**页面。它可显示 Websense 软件的运行状态，还可显示自子夜以来网络中的筛选活动图表。（请参阅*今天：从子夜以来的运行状况、安全和数值情况*，第 20 页。）
- **历史**页面最多可显示 30 天内的网络筛选活动图表，但具体取决于日志数据库中的信息量。这些图表不包括今天的活动。（请参阅*历史：最近 30 天*，第 23 页。）
- **演示报告**和**调查报告**可为生成、自定义和计划报告提供多种选项。请参阅*报告概述*，第 82 页，以了解更多信息。

如果您的组织将 Websense Manager 安装在 Linux 服务器上，或者选择 Websense Explorer for Linux 报告程序（而未选择在 Windows 上运行的报告组件），则报告选项不会显示在 Websense Manager 中。而“今天”和“历史”页面中也不会显示 Internet 筛选图表。请参阅 *Explorer for Linux 管理员指南*，以了解安装程序和运行报告的有关信息。

报告概述

相关主题：

- *使用报告以评估筛选策略*，第 81 页
- *演示报告*，第 84 页
- *调查报告*，第 100 页
- *访问自我报告*，第 121 页

除了出现在“今天”和“历史”页上的图表之外，Websense 软件还提供 2 个报告选项：演示报告和调查报告。

注意

在使用委派管理的组织中，部分管理员可能无法访问所有报告功能。请参阅*委派管理*，第 197 页。

演示报告可为您提供报告定义列表。其中一些是列表报告，还有一些则结合了条形图和表格。要生成演示报告：

1. 请从列表中选择一个报告。
2. 单击**运行**。
3. 选择日期范围。
4. 单击**立即运行**。

除了可生成预定义图表之外，您还可复制这些图表并应用自定义报告筛选器，以识别需要包括的指定客户端、类别、协议和操作。将常用的报告定义勾选为收藏报告，以便更快捷地找到它们。

您可计划任何演示报告，令其在特定时间运行或重复循环运行。请参阅*演示报告*，第 84 页，以了解完整的详细信息。

调查报告可令您以互动方式浏览日志数据。主页面将按风险级别显示活动的摘要式条形图。单击页面上的不同元素可更新图表或获得数据的不同视图。

- 单击风险级别名称，然后选择一个与该风险级别相关的更精确级别的详细信息。例如，您可选择按用户显示“法律责任”风险级别的活动。
- 在生成的表格上单击用户名，可查看该用户的更多详细信息。
- 从 **Internet 用户**列表中选择不同选项可更改摘要条形图。
- 填写条形图上方的字段，可一次显示两种级别的信息。例如，从类别的摘要图表开始时，您可依次选择 **10**、**用户**和 **5**，以显示前 10 个类别中前 5 名用户的活动。
- 单击条或数字可打开该项目（风险级别、类别、用户或其他）的详细报告。

- 单击**收藏报告**可保存具有特殊用途的报告便于日后使用，或生成以前保存的收藏报告。

您可有无限种可用操作。请参阅*调查报告*，第 100 页，以了解查看 Internet 使用数据的多种方法的详细信息。

Internet 浏览时间是什么？

相关主题：

- *数据库作业*，第 270 页
- *配置 Internet 浏览时间选项*，第 274 页

您可根据 Internet 浏览时间（IBT，即个人访问网站所用时间）生成演示报告和调查报告。没有任何一种软件程序可告知某个人自打开某一特定站点起查看该站点所用的确切时间。有些人可能打开站点，查看几秒钟后就去打工作电话，然后又请求另一个站点。还有一些人可能会花几分钟仔细阅读每个站点，并继续阅读另一个网站。

Websense 软件中包含一个日志数据库作业，可利用基于某些可配置值的公式来计算 Internet 浏览时间 (IBT)。该作业一天运行一次，因此浏览时间信息会滞后于实际的日志数据。

为计算浏览时间，用户一打开浏览器就会开始 Internet 会话。只要用户至少每 3 分钟请求其他网站一次， Internet 会话就会继续。（这一默认读取时间阈值可进行配置。）

若用户请求其他网站前已超过 3 分钟，则 Internet 会话终止。Websense 软件将计算会话总时间，从第一次请求的时间开始，直到最后一次请求 3 分钟后为止。

如果用户超过 3 分钟后又开始另一个请求，则开始新的会话。通常，一名用户的浏览时间每天都会由多个会话组成。

请参阅*数据库作业*，第 270 页和*配置 Internet 浏览时间选项*，第 274 页，以了解关于 Internet 浏览时间作业和相关配置选项的有关信息。

演示报告

相关主题：

- *复制演示报告*，第 86 页
- *复制演示报告*，第 86 页
- *使用 “收藏报告”*，第 92 页
- *生成演示报告*，第 93 页
- *计划演示报告*，第 94 页
- *查看计划作业列表*，第 98 页

报告 > 演示报告页面将显示一个预定义图表和列表报告的列表，每个图表和报告均显示了日志数据库中的具体信息（请参阅*日志数据库概述*，第 270 页）。从该报告编录中选择一个报告，可显示其简要说明。

您可复制预定义报告并自定义报告筛选器，以指定其需要包括的客户端、类别、协议和操作。常用的报告可被标记为收藏报告，以便更快捷地找到它们。

您可立即运行任何报告，或将选择的报告计划为延迟运行或定期运行。选择输出格式，并将计划的报告分发给选择收件人组。

如果您从“演示报告”页面中直接生成 HTML 格式的报告，则该报告在您转到另一个页面时不会被保存。如果您生成 PDF 或 XLS 格式的报告并立即查看，则该报告在您关闭查看程序（Adobe Reader 或 Microsoft Excel）时不会被保存。

或者，您可选择保存 PDF 或 XLS 文件（而不是立即显示文件），或在查看程序中使用“保存”选项。在这种情况下，请务必定期删除或移动报告文件，以避免磁盘空间不足的问题。

计划的报告将会被自动保存到以下目录：

```
< 安装路径 >\ReportingOutput
```

默认安装路径为 C:\Program Files\Websense。

当计划的演示报告已运行时，报告文件将以名为 **presentationreport_0** 的电子邮件附件发送给收件人。文件名中的数字将根据所附报告数量的增加而递增。请注意，附件名与 ReportingOutput 目录中存储的文件名不匹配。要查找此目录中的特定报告，请搜索计划作业运行当天创建的文件。

报告将在 15 天后从 ReportingOutput 目录中自动删除。如果您想长期保留报告，请将它们包括入您的备份例程中，或计划它们，并将已通过电子邮件发送的文件保存到可长期存储的位置。

根据您每天生成的报告数量，报告文件可能会占据相当大的磁盘空间。请确保 Websense Manager 计算机上有足够的磁盘空间。如果 ReportingOutput 目录在自动删除文件之前所占据的空间过大，您可手动删除文件。

Websense 软件可按您选择的格式生成报告：PDF （Adobe Reader）、 XLS（Microsoft Excel）或 HTML。如选择 HTML 格式，则报告将在 Websense Manager 内容窗格中显示。此类报告不能打印，也不能保存为文件。要打印报告或将其保存为文件，请选择 PDF 或 XLS 输出格式。

如选择 PDF 或 XLS 格式，您可将报告文件保存到磁盘或在单独窗口中显示报告文件。

重要

要以 PDF 格式显示演示报告，则必须在用于访问 Websense Manager 的计算机上安装 Adobe Reader v7.0 或更高版本。

要以 XLS 格式显示演示报告，则必须在用于访问 Websense Manager 的计算机上安装 Microsoft Excel 2003 或更高版本。

在“演示报告”页面上通过“报告编录”导航，并选择您关注的报告。然后，使用页面上的控件运行报告，创建副本以用于自定义报告筛选器和进行更多操作。

按钮	操作
仅显示收藏报告	选择此选项可将“报告编录”限制为仅显示标记为“收藏报告”的报告。 取消选中此选项，则可恢复完整的报告列表。
编辑报告筛选器	此选项仅在选择预定义报告副本时才可用，它可帮助您选择要包括入报告的特定类别、协议、用户和操作。请参阅*复制演示报告*，第 86 页。
复制	复制选择的报告并将其作为自定义报告添加到“报告编录”中。请参阅*复制演示报告*，第 86 页。 选择自定义报告，然后单击**编辑报告筛选器**设置它的具体参数。
收藏报告	将选择的报告勾选为“收藏报告”或删除“收藏报告”标记。请参阅*使用“收藏报告”*，第 92 页。 “报告编录”会在任何标记为“收藏报告”的报告名旁显示一个星号。使用**仅显示收藏报告**复选框可控制在“报告编录”中显示的报告类别。
删除	从“报告编录”中删除选择的报告副本。您无法删除随软件一起安装的预定义报告。 如果已删除的报告出现在任何计划作业中，它将继续和该作业一起生成。
运行	您可在设置日期范围和输出格式后生成选择的报告。请参阅*生成演示报告*，第 93 页。 要控制自定义报告 （预定义报告的副本）的其他方面，请参阅*复制演示报告*，第 86 页。 要计划报告使其在其他时间运行或根据计划重复运行，请单击 “计划程序”。

该页面上的按钮可为您提供演示报告的其他选项。

按钮	操作
作业队列	将显示一个页面，其上列出了已创建的计划作业和每个作业的状态。请参阅*查看计划作业列表*，第 98 页。
计划程序	可令您定义包含一个或多个报告的作业，使其在指定时间运行或根据计划重复运行。请参阅*计划演示报告*，第 94 页。

复制演示报告

相关主题：

- *复制演示报告*，第 86 页
- *演示报告*，第 84 页

初始化时，**演示报告**页面会显示“报告编录”，列出与软件一起安装的所有预定义报告。您可通过选择报告然后单击“运行”在指定时间段生成任何此类报告。

这些预定义报告也可作为模板，从而被复制以创建自定义报告筛选器。创建报告筛选器可控制某些元素，例如当您从副本生成报告时需要包括的用户、类别、协议和操作。

复制报告并编辑报告筛选器后，您可复制新报告，从而根据该副本创建变量。

1. 选择“报告编录”中的任何报告。
2. 单击**复制**。

   则“报告编录”中将显示重复的报告名称以及标识其为副本的附注代码。
3. 在“报告编录”中选择副本，然后单击**编辑报告筛选器**可修改报告的元素。请参阅*复制演示报告*，第 86 页。

定义报告筛选器

相关主题：

- *复制演示报告*，第 86 页
- *生成演示报告*，第 93 页

报告筛选器可帮助您控制报告中包括的信息内容。例如，您可选择将报告限制到指定客户端、类别、风险级别或协议，或者甚至是选择的筛选操作（允许、阻止等等）。您也可为“报告编录”中的项目提供新名称和描述、指定要显示的自定义徽标，并通过报告筛选器设置其他常规选项。

> **注意**
>
> 使用自定义徽标需要在您定义报告筛选器前做一些准备工作。您必须以支持的图形格式创建所需图形并将文件保存到相应位置。请参阅 *自定义报告徽标*，第 91 页。

筛选器中可用的特定选项依选择的报告而异。例如，如果您已选择组信息报告，如 “请求的最常见被阻止组”，则您可控制在报告中显示的组，但不能选择单个用户。

预定义报告的筛选器不能更改。您可针对预定义报告的副本编辑筛选器：

1. 选择 “报告编录”中的报告。

   如果 “编辑报告筛选器”按钮被禁用，请继续步骤 2。

   如果 “编辑报告筛选器”按钮已启用，请跳到步骤 3。

2. 单击**复制**制作副本以供您自定义使用。

   则 “报告编录”中将显示重复的报告名称以及标识其为副本的附注代码。

3. 单击**编辑报告筛选器**按钮。

   打开 “报告筛选器”页面，该面将包含管理报告的不同元素的单独选项卡。在每个选项卡上选择所需项目，然后单击**下一个**移动到下一个选项卡。有关详细信息，请参阅：

   - *选择报告的客户端*，第 87 页
   - *选择报告的类别*，第 88 页
   - *选择报告的协议*，第 89 页
   - *选择报告的操作*，第 90 页
   - *设置报告选项*，第 90 页

4. 在**确认**选项卡上，选择除保存报告筛选器之外的其他操作，运行报告还是计划报告。请参阅 *确认报告筛选器定义*，第 92 页。

选择报告的客户端

相关主题：

- *选择报告的类别*，第 88 页
- *选择报告的协议*，第 89 页
- *选择报告的操作*，第 90 页
- *设置报告选项*，第 90 页
- *确认报告筛选器定义*，第 92 页

演示报告 > 报告筛选器页面的**客户端**选项卡可帮助您控制报告中需包括的客户端。在每个报告中，您只能选择一种类型的客户端。例如，在同一个报告中，您不能同时选择用户和组。

当报告定义指定特定的客户端类型时，您可选择该类型的客户端或代表更大分组的客户端。例如，如果您正为以“请求的最常见被阻止组”为基础的报告定义筛选器，您可为报告选择组、域或组织单位，但不能选择单个用户。

如果您想报告所有相关客户端，则无需在此选项卡上作出选择。

1. 从下拉列表中选择一种客户端类型。
2. 从**限制搜索**列表中设置搜索结果的最大数量。

   根据您组织中的流量，日志数据库中可能会有大量的用户、组或域。此选项可用于管理结果列表的长度和显示搜索结果所需的时间。
3. 输入一个或多个搜索字符，然后单击**搜索**。

   使用星号 (*) 作为通配符，以代表缺少的字符。例如，输入 J*n 可能会返回 Jackson、 Jan、 Jason、 Jon、 John 等搜索结果。

   请仔细定义您的搜索字符串，以确保所有所需结果都会包括在限制搜索的数字之内。
4. 突出显示结果列表中的一个或多个项，并单击右侧的箭头按钮 （>），将它们移至**选择的**列表。
5. 根据需要重复步骤 2-4 以执行其他搜索以及将更多客户端添加到选择的列表。
6. 完成选择之后，请单击**下一步**打开 “类别”选项卡。请参阅*选择报告的类别*，第 88 页。

选择报告的类别

相关主题：

- *选择报告的客户端*，第 87 页
- *选择报告的协议*，第 89 页
- *选择报告的操作*，第 90 页
- *设置报告选项*，第 90 页
- *确认报告筛选器定义*，第 92 页

演示报告 > 报告筛选器页面的**类别**选项卡可帮助您根据类别或风险级别控制包括在报告内的信息。请参阅*风险级别*，第 36 页。

如果您想报告所有相关类别或风险级别，则无需在此选项卡上作出选择。

1. 选择分类：**类别**或**风险级别**。

   展开父类别可显示其子类别。展开风险级别可查看当前分配到该风险级别的类别列表。

如果相关报告属于特定的风险级别，则只有其代表的相关风险级别和类别才可用于选择。

> **注意**
> 如果您选择报告中指定的风险级别的类别子集，请考虑修改报告标题以反映您的选择。

2. 勾选每个要报告的类别或风险级别的复选框。

   使用列表下方的**全选**和**全部清除**按钮可最小化所需单个选择的数量。
3. 单击右侧的箭头按钮 （>），将您的选择移动到**选择的**列表。

   勾选风险等级时，单击右侧的箭头可将所有相关类别放入已选择的列表。
4. 完成所有选择后，请单击**下一步**打开 “协议”选项卡。请参阅*选择报告的协议*，第 89 页。

选择报告的协议

相关主题：

- *选择报告的客户端*，第 87 页
- *选择报告的类别*，第 88 页
- *选择报告的操作*，第 90 页
- *设置报告选项*，第 90 页
- *确认报告筛选器定义*，第 92 页

演示报告 > 报告筛选器页面的**协议**选项卡可帮助您控制报告中需包括的协议。

如果您想报告所有相关协议，则无需在此选项卡上作出选择。

1. 展开组名旁带有图标的协议组并将其折叠。
2. 勾选每个要报告的协议的复选框。

   使用列表下方的**全选**和**全部清除**按钮可最小化所需单个选择的数量。
3. 单击右侧的箭头按钮 （>），将您的选择移动到**选择的**列表。
4. 完成所有选择后，请单击**下一步**打开 “操作”选项卡。请参阅*选择报告的操作*，第 90 页。

选择报告的操作

相关主题：

- *选择报告的客户端*，第 87 页
- *选择报告的类别*，第 88 页
- *选择报告的协议*，第 89 页
- *设置报告选项*，第 90 页
- *确认报告筛选器定义*，第 92 页

演示报告 > 报告筛选器页面的**操作**选项卡可帮助您控制报告中需包括的确切筛选操作（例如被受限访问筛选器允许、按定额阻止）。如报告指定特定类型的操作，例如“已阻止”，则您将受到限制，只可为报告选择该类型的操作。

如果您想报告所有相关操作，则无需在此选项卡上作出选择。

1. 展开组名旁带有图标的操作组并将其折叠。
2. 勾选每个要报告的操作的复选框。

   使用列表下方的**全选**和**全部清除**按钮可最小化所需单个选择的数量。
3. 单击右侧的箭头按钮（>），将您的选择移动到**选择的**列表。
4. 完成所有选择后，请单击**下一步**打开“选项”选项卡。请参阅 *设置报告选项*，第 90 页。

设置报告选项

相关主题：

- *自定义报告徽标*，第 91 页
- *选择报告的客户端*，第 87 页
- *选择报告的类别*，第 88 页
- *选择报告的协议*，第 89 页
- *选择报告的操作*，第 90 页
- *设置报告选项*，第 90 页
- *确认报告筛选器定义*，第 92 页

使用“演示报告”>“编辑报告筛选器”页面的**选项**选项卡可配置报告的各个方面。

1. 修改显示在报告编录中的**报告编录名称**。此名称最多可包含 85 个字符。

   此名称本身不会出现在报告上；它仅用于识别“报告编录”中报告格式和筛选器的唯一组合。

2. 修改显示在报告上的**报告标题**。此标题最多可包含 85 个字符。
3. 修改出现在 “报告编录”中的**描述**。此描述最多可包含 336 个字符。

   此描述可帮助您识别 “报告编录”中报告格式和筛选器的唯一组合。
4. 选择出现在报告上的徽标。

   相应目录中的所有支持图像文件都将列出。请参阅 *自定义报告徽标*，第 91 页。
5. 勾选**另存为收藏报告** 复选框，将列出的报告标识为 “收藏报告”。

   “报告编录”将在收藏报告旁显示一个星号。您可在 “报告编录”页面上选择**仅显示收藏报告**以减少列出的报告数量，以便您更快捷地找到特定报告。
6. 勾选**仅显示顶部**复选框，然后输入介于 1 到 20 之间的数字，可限制报告的项目数量。

   此选项仅在选择的报告格式为 Top N 报告 （旨在显示有限数量的项目）时才会出现。受限制的项目取决于报告本身。例如，对于 “最常访问类别”报告，该项可确定报告的类别数量。
7. 完成所有选择后，请单击**下一步**打开 “确认”选项卡。请参阅 *确认报告筛选器定义*，第 92 页。

自定义报告徽标

预定义演示报告将在左上角显示 Websense 徽标。复制预定义报告并定义其报告筛选器时，可选择不同的徽标。

1. 您可用以下格式之一创建图像文件：

   - .bmp
   - .gif
   - .jfif
   - .jpe
   - .jpg
   - .jpeg
   - .png
   - .ttf

2. 图像文件名 （包括扩展名）最多包含 25 个字符。
3. 将图像文件放入以下目录：

   < 安装路径 >\Manager\ReportingTemplates\images

   默认安装路径为 C:\Program Files\Websense。

此目录中的所有支持图像文件将自动显示在 “报告筛选器”页面的 “选项”选项卡上的下拉菜单中。图像会自动缩放以适应分配给徽标的空间。（请参阅 *设置报告选项*，第 90 页。）

注意

请勿从此目录删除报告筛选器中处于活动状态的图像。如果指定的徽标文件丢失，则报告无法生成。

确认报告筛选器定义

相关主题：

- *选择报告的客户端*，第 87 页
- *选择报告的类别*，第 88 页
- *选择报告的协议*，第 89 页
- *选择报告的操作*，第 90 页
- *设置报告选项*，第 90 页

演示报告 > 报告筛选器页面的**确认**选项卡可显示将在 “报告编录” 中出现的名称和描述，以便您选择如何进行后续操作。

1. 查看**名称**和**描述**。

   如需任何更改，请单击**上一步**返回 “选项” 选项卡以进行更改。（请参阅*设置报告选项*，第 90 页。）

2. 指明您要如何进行：

选项	描述
保存	保存报告筛选器并返回“报告编录”。请参阅*演示报告*，第 84 页。
保存并运行	保存报告筛选器并打开 “运行报告” 页面。请参阅*生成演示报告*，第 93 页。
保存和计划	保存报告筛选器并打开 “计划报告” 页面。请参阅*计划演示报告*，第 94 页。

3. 单击**完成**以执行步骤 2 中作出的选择。

使用 “收藏报告”

相关主题：

- *演示报告*，第 84 页
- *生成演示报告*，第 93 页
- *计划演示报告*，第 94 页

您可将任何演示报告 （预定义或自定义）勾选为收藏报告。使用此选项可帮助您标识最常生成且需在 “报告编录” 中快速查找的报告。

1. 在**演示报告**页面，突出显示您经常生成或需要快速查找的报告。

2. 单击**收藏报告**。

   列表中收藏报告名旁会出现一个星号，以便您在显示所有报告时可迅速识别它们。

3. 勾选“报告编录”上方的**仅显示收藏报告**复选框，可限制列表仅显示标记为“收藏报告”的报告。取消勾选此选项，则可恢复完整的报告列表。

如需更改，且收藏报告的使用不再频繁，您可删除“收藏报告”标记。

1. 突出显示带有“收藏报告”星号的报告。
2. 单击**收藏报告**。

   “报告编录”中的星号将从报告名旁删除。现在，如选择**仅显示收藏报告**，则该报告会从列表中消失。

生成演示报告

相关主题：

- *演示报告*，第 84 页
- *计划演示报告*，第 94 页

生成单一报告需包括以下几个步骤。

注意

生成 PDF 格式的报告之前，请确保用于访问 Websense Manager 的计算机上已安装 Adobe Reader v7.0 或更高版本。

生成 XLS 格式的报告之前，请确保用于访问 Websense Manager 的计算机上已安装 Microsoft Excel 2003 或更高版本。

如未安装相应软件，您可选择保存文件。

要创建作业，使一个或多个报告可通过演示报告计划功能一次或重复循环运行，请参阅*计划演示报告*，第 94 页。

1. 在**演示报告**页面上，突出显示“报告编录”中的报告，然后单击**运行**。
2. 选择报告数据的**开始日期**和**结束日期**。
3. 选择报告的**输出格式**。

格式	描述
PDF	便携式文档格式。PDF 文件需在 Adobe Reader 中查看。
HTML	HyperText Markup 语言。 HTML 文件可通过 Internet Explorer 或 Firefox 浏览器直接查看。
XLS	Excel 电子表格。XLS 文件需在 Microsoft Excel 中查看。

4. 如果您已选择 **Top N** 报告，请选择要报告的项目数量。
5. 单击**运行**。

   HTML 报告将出现在内容窗格中。如果您已选择 PDF 或 XLS 输出格式，您可选择在单独窗口中打开报告或者将报告保存到磁盘中。
6. 要打印报告，请使用打印选项，它是显示报告的程序的一部分。

   要获得最佳效果，请生成 PDF 或 XLS 输出格式以便打印。然后，使用 Adobe Reader 或 Microsoft Excel 各自的打印选项。

您可使用 Adobe Reader 或 Microsoft Excel 中的 “保存” 功能将报告以 PDF 或 XLS 的输出格式进行保存。

计划演示报告

相关主题：

- *演示报告*，第 84 页
- *生成演示报告*，第 93 页
- *查看计划作业列表*，第 98 页
- *复制演示报告*，第 86 页

您可根据需要运行演示报告，或者使用**演示报告 > 计划程序**页面以创建作业，从而定义计划以用于运行一个或多个报告。

由计划作业生成的报告将通过电子邮件分发给一个或多个收件人。创建计划作业时，请考虑您的电子邮件服务器是否能够处理所附报告文件的大小和数量。

要访问 “计划程序”：

- 单击 “演示报告” 页面顶部 （“报告编录” 上方）的**计划程序**按钮。
- 针对报告添加或编辑报告筛选器时，请选择 “确认” 选项卡中的**保存和计划**，然后单击**完成**。（请参阅*复制演示报告*，第 86 页。）
- 单击 “作业队列” 页面上的作业名称链接可编辑作业。
- 单击 “作业队列” 页面上的**添加**可创建新作业。

“计划作业” 页面包括几个选项卡，可用于选择要运行的报告；此外还包括用于运行报告的计划。有关详细信息，请参阅：

- *设置计划*，第 95 页
- *选择要计划的报告*，第 96 页
- *选择输出选项*，第 97 页
- *选择日期范围*，第 96 页
- *选择输出选项*，第 97 页

创建作业后，您可查看显示作业状态和其他有用信息的作业列表。请参阅*查看计划作业列表*，第 98 页。

设置计划

相关主题：

- *计划演示报告*，第 94 页
- *选择要计划的报告*，第 96 页
- *选择输出选项*，第 97 页
- *选择日期范围*，第 96 页

在演示报告 > 计划程序页面的**计划**选项卡上，定义要一次或重复循环运行的报告作业。

> **注意**
> 建议您在不同日期或不同时间计划报告作业，以避免因日志数据库负荷过大而导致降低记录和互动报告的性能。

1. 输入可唯一标识此计划作业的**作业名称**。
2. 选择作业的**重复模式**和**重复选项**。可用的特定选项取决于所选模式。

模式	选项
一次	输入运行作业的确切日期，或单击图标从日历中选择。
每日	无其他可用的重复选项。
每周	勾选运行作业的一周中每一天的复选框。
每月	输入运行作业的月份中的日期。日期必须为介于 1 到 31 之间的数字，且必须用逗号隔开 （1， 10， 20）。 要在每月的连续日期内运行作业，请输入开始日期和结束日期，中间用连字符隔开 （3-5）。

3. 在**计划时间**中，设置运行作业的开始时间。

   作业将根据运行 Websense Manager 的计算机上设置的时间开始运行。

> **注意**
> 要在今天开始生成计划报告，请选择一个较晚的时间，以便您在开始时间之前有足够的时间完成作业定义。

4. 在**计划期间**中，选择开始作业的日期和结束作业的选项。

选项	描述
没有结束日期	作业将根据已建立的计划继续无期限运行。 要在以后某个时候中止作业，请编辑或删除作业。请参阅*查看计划作业列表*，第 98 页。
在该日期之后结束	选择运行作业的次数。达到该重复次数后，作业将不再运行，但仍会保留在“作业队列”中，直到您删除为止。请参阅*查看计划作业列表*，第 98 页。
在该日期之前结束	设置作业停止运行的日期。在该日期以及该日期之后它将不再运行。

5. 单击**下一步**打开“报告”选项卡。请参阅*选择要计划的报告*，第 96 页。

选择要计划的报告

相关主题：

- *计划演示报告*，第 94 页
- *设置计划*，第 95 页
- *选择输出选项*，第 97 页
- *选择日期范围*，第 96 页

使用演示报告 > 计划程序页面的**选择报告**选项卡可选择作业的报告。

1. 在“报告编录”树中突出显示此作业的报告。
2. 单击右侧的箭头按钮 (>)，将该报告移动到**选择的**列表。
3. 重复步骤 1 和 2，直到此作业的所有报告都出现在**选择的**列表中。
4. 单击**下一步**打开“日期范围”选项卡。请参阅*选择日期范围*，第 96 页。

选择日期范围

相关主题：

- *计划演示报告*，第 94 页
- *设置计划*，第 95 页
- *选择要计划的报告*，第 96 页
- *选择输出选项*，第 97 页

使用演示报告 > 计划程序页面的**日期范围**选项卡可选择作业的日期范围。可用的选项取决于您选择的**日期范围**。

日期范围	描述
所有日期	报告将包括日志数据库中的所有可用日期，无需其他项。 此选项用于重复作业时，可能会在单独的运行中出现重复的报告信息。
具体日期	选择此作业中报告的确切开始日期（**从**）和结束（**到**）日期。 此选项尤其适合于仅运行一次的作业，也可在重复报告中重复计划结果。
相对日期	使用下拉列表选择要报告的时间段数量（“本时间段”、“最近 1 个时间段”、“最近 2 个时间段”等等）以及时间段类型（“天”、“周”或“月”）。例如，作业可能涵盖“最近 2 周”或“本月”。 “周”代表从周日至周六的日历周。“月”代表日历月。例如，选择“本周”可生成从周日到今天的报告；选择“本月”可生成从 1 号到今天的报告；选择“最近 1 周”可生成从上周日到周六的报告，以此类推。 此选项尤其适合于重复运行的作业。它可令您管理每份报告上出现的数据数量，并尽量减少单独运行中报告上的重复数据。

设置作业的日期范围后，单击**下一步**显示“输出”选项卡。请参阅*选择输出选项*，第 97 页。

选择输出选项

相关主题：

- *计划演示报告*，第 94 页
- *设置计划*，第 95 页
- *选择要计划的报告*，第 96 页
- *选择日期范围*，第 96 页

选择作业的报告后，使用**输出**选项卡可选择输出格式和分发选项。

1. 选择已完成报告的文件格式。

格式	描述
PDF	便携式文档格式。收件人必须安装 Adobe Reader v7.0 或更高版本才可查看 PDF 报告。
XLS	Excel 电子表格。收件人必须安装 Microsoft Excel 2003 或更高版本才可查看 XLS 报告。

2. 输入电子邮件地址以便分发报告。

   每行输入一个电子邮件地址。
3. 根据需要勾选**自定义电子邮件主题和正文**复选框。然后，输入此作业分发电子邮件的自定义**主题**和**正文**文本。
4. 单击**保存作业**以保存和执行作业定义，并显示“作业队列”页面。
5. 查看此作业和任何其他的计划作业。请参阅*查看计划作业列表*，第 98 页。

查看计划作业列表

相关主题：

- *演示报告*，第 84 页
- *计划演示报告*，第 94 页
- *选择输出选项*，第 97 页
- *计划调查报告*，第 117 页

演示报告 > **作业队列**页面将列出针对演示报告创建的计划作业。此列表给出了每个作业的状态以及作业的基本信息（如运行频率）。您可从此页面添加和删除计划作业、临时暂停作业以及其他更多操作。

（要查看调查报告的计划作业，请参阅*管理计划的调查报告作业*，第 119 页。）

此列表将为您提供每项作业的以下信息。

列	描述
作业名称	创建作业时分配的名称。
情况	其中包括以下情况之一： • “已启用”表示根据已建立的重复模式运行的作业。 • “已禁用”表示处于非活动状态且不运行的作业。
递归	针对此作业设置的重复模式（一次、每日、每周、每月）。
历史	单击**详细信息**链接可打开选择作业的“作业历史”页面。请参阅*查看作业历史*，第 99 页。
下一个计划	下一次运行的日期和时间。
所有者	计划作业的管理员用户名。

使用此页面上的选项可对作业进行管理。某些按钮需在要包括的每项作业名称旁勾选复选框才可启用。

选项	描述
作业名称链接	打开“计划程序”页面，您可在此编辑作业定义。请参阅 *计划演示报告*，第 94 页。
添加作业	打开“计划程序”页面，您可在此定义新作业。请参阅 *计划演示报告*，第 94 页。
删除	从“作业队列”中删除列表中所有被选中的作业。一旦作业被删除，将无法恢复。 要暂时停止运行某项特定作业，请使用**禁用**按钮。
立即运行	立即开始运行列表中被选中的作业。该运行是对定期计划运行的补充。
启用	重新激活列表中被选中的已禁用作业。此作业将根据已建立的计划开始运行。
禁用	中止运行列表中被选中的已启用作业。使用此临时暂停功能将令您可在日后恢复该作业。

查看作业历史

相关主题：

- *计划演示报告*，第 94 页
- *查看计划作业列表*，第 98 页

使用**演示报告 > 作业队列 > 作业历史**页面，可查看有关最近几次尝试运行选择作业的信息。此页面将单独列出每份报告，并提供以下信息。

列	描述
报告名称	报告上打印的标题。
开始日期	报告开始运行的日期和时间。
结束日期	报告完成的日期和时间。
状态	用于指示报告是否成功或是失败。
消息	关于作业的相关信息，例如报告是否已通过电子邮件成功发送。

调查报告

相关主题：

- *摘要报告*，第 101 页
- *多级摘要报告*，第 104 页
- *灵活的详细报告*，第 105 页
- *用户活动详细信息报告*，第 109 页
- *标准报告*，第 113 页
- *收藏调查报告*，第 114 页
- *计划调查报告*，第 117 页
- *异常值报告*，第 119 页
- *输出到文件*，第 120 页
- *数据库连接与报告默认*，第 280 页

使用**报告 > 调查报告**页面可用互动方式分析 Internet 筛选活动。

初始化时，“调查报告”主页面将根据风险级别显示活动的报告摘要。单击可用链接和元素可在摘要报告视图中进行操作，以查看您所关注的区域，并大致了解您组织的 Internet 使用情况。请参阅*摘要报告*，第 101 页。

多级摘要报告 （请参阅*多级摘要报告*，第 104 页）和灵活的详细报告 （请参阅*灵活的详细报告*，第 105 页）可帮助您从不同角度分析信息。

从页面顶部的链接可访问其他报告视图和调查报告功能。请参阅以下表格，以了解可访问的链接和功能列表。（并非所有页面上的所有链接都可用。）

选项	操作
用户每日/月	显示可供您定义指定用户的活动报告的对话框，涵盖范围可为一天或一个月。更多信息，请参阅*用户活动详细信息报告*，第 109 页。
标准报告	显示预定义报告列表，以便您迅速查看特定组合的数据。请参阅*标准报告*，第 113 页。
收藏报告	可帮助您将当前报告保存为“收藏报告”，并显示您可生成或计划的现有收藏报告列表。请参阅*收藏调查报告*，第 114 页。
作业队列	显示计划的调查报告作业列表。请参阅*计划调查报告*，第 117 页。
查看异常值	显示报告，以指出与平均值差别很大的 Internet 使用情况。请参阅*异常值报告*，第 119 页。

选项	操作
选项	显示可为报告选择不同日志数据库的页面。选项页面也可帮助您自定义某些报告功能，例如摘要报告初始显示的时间段和详细报告的默认列。请参阅*数据库连接与报告默认*，第 280 页。
	单击“搜索”字段右侧的按钮，可将当前报告导出到与 Microsoft Excel 兼容的电子表格文件。 系统将提示您打开或保存文件。要打开文件，则必须安装 Microsoft Excel 2003 或更高版本。请参阅*输出到文件*，第 120 页。
	单击“搜索”字段右侧的按钮，可将当前报告导出到与 Adobe Reader 兼容的 PDF 文件。 系统将提示您打开或保存文件。要打开文件，则必须安装 Adobe Reader version 7.0 或更高版本。请参阅*输出到文件*，第 120 页。

请记住，报告仅限于提供已在“日志数据库”中记录的信息。如果针对用户名、IP 地址或选择的类别禁用记录（请参阅*配置 Filtering Service 以进行日志记录*，第 257 页），则相应信息不会被包括在报告中。同样，如果针对特定协议禁用记录（请参阅*编辑协议筛选器*，第 46 页），则这些协议的请求也不可用。如果您希望报告显示域名（www.domain.com）和通往域中特定页面的路径（/products/productA），则必须记录完整的 URL（请参阅*配置完整 URL 记录*，第 273 页）。

Websense 调查报告将受到运行 Websense Manager 的计算机的处理器、可用内存以及一些网络资源的限制。生成一些大容量报告可能需要较长的时间。进度消息包括将报告保存为“收藏报告”的选项，以便您可计划报告使其在其他时间运行。请参阅*计划调查报告*，第 117 页。

摘要报告

相关主题：

- *多级摘要报告*，第 104 页
- *灵活的详细报告*，第 105 页
- *用户活动详细信息报告*，第 109 页
- *标准报告*，第 113 页
- *收藏调查报告*，第 114 页
- *计划调查报告*，第 117 页
- *异常值报告*，第 119 页
- *输出到文件*，第 120 页

初始化时，调查报告页面将按风险级别提供所有用户使用情况的摘要报告，以显示日志数据库中的当天活动。此初始条形图按点击量（站点被请求的次数）进行计算。要配置此初始摘要报告的时间段，请参阅*数据库连接与报告默认*，第 280 页。

单击页面上的多个链接和可用选项可迅速更改报告的信息或向下搜索报告的详细信息。

1. 从以下**衡量标准**列表的选项中选择其一。

选项	描述
点击量	URL 被请求的次数。 根据 Log Server 的配置方式，这里显示的数字可能是真正的点击量，记录了所请求网站的每一个独立元素；也可能只是访问量，将网站的不同元素合并为单一的日志记录。请参阅*配置日志缓存文件*，第 263 页。
带宽 [KB]	包括在用户的初始请求和网站的响应中包括的所有数据量（以 KB 为单位），是发送值和接收值的总和。 请记住，某些集成产品不向 Websense 软件发送信息，例如 Check Point FireWall-1 和 Cisco PIX Firewall。如果您的集成产品不发送此信息，且 Websense Network Agent 已安装，请激活相应 NIC 的**记录 HTTP 请求**选项以启用带宽信息报告。请参阅*配置 NIC 设置*，第 292 页。
已发送 [KB]	Internet 请求发送的 KB 数。此数字代表已传输的数据量，它可以是简单的 URL 请求，或是在用户注册网站时提交的重要内容。
已接收 [KB]	响应请求时接收的 KB 数。其中包括构成站点的所有文本、图形和脚本。 对于已阻止的站点而言， KB 数根据创建日志记录的软件不同而各异。当 Websense Network Agent 进行记录时，已阻止站点所接收的字节数代表 Websense 阻止页面的大小。 如果日志记录由 Websense Security Gateway 创建，则作为实时扫描的结果，收到的 KB 数将代表已扫描页面的大小。请参阅*分析带实时选项的内容*，第 123 页，以了解更多有关实时扫描的信息。 如果由其他集成产品创建日志记录，则已阻止站点所接收的 KB 可能为零（0），可能代表阻止页面的大小，也可能是从请求的站点获得的值。
浏览时间	浏览站点所用时间的估计值。请参阅*Internet 浏览时间是什么？*，第 83 页。

2. 从报告上方的 **Internet 用户**列表中选择一个选项，可更改报告的原始分组。

   选项将根据日志数据库的内容和特定网络考量不同而各异。例如，如果日志数据库中只有一个组或域，则“组”和“域”不会出现在此列表中。同样，如果用户过多（大于 5,000）或者组过多（大于 3,000），则这些选项也不会出现。（您可对此类限制中的其中一些进行配置。请参阅*显示和输出选项*，第 282 页。）

3. 单击左列中的名称（或名称旁边的箭头）可显示选项列表，例如按用户、按域或按操作排序。

   列出的选项类似于“ Internet 用户”下面列出的内容，可自定义成为含义丰富的当前显示内容的子集。

   > **注意**
   >
   > 有时，诸如“用户”或“组”等的选项会显示为红字。这种情况下，选择该选项可以较慢的速度生成容量极大的报告。您可在选择该选项前考虑进一步向下搜索，以获取更多详细信息。

4. 选择此类选项中的其中之一可生成新的摘要报告，以显示相关项的特定信息。

   例如，在“风险级别”摘要报告上，单击“法律责任”风险级别下面的“按用户”，可生成 “法律责任”风险级别中每位用户的活动报告。

5. 单击左列中的新项，然后选择一个选项可查看该特定项目的详细信息。
6. 使用列标题旁的箭头可更改报告的排序方式。
7. 使用图表上方的以下选项，可控制摘要报告。然后，通过单击新报告的元素深入了解相关详细信息。

选项	操作
报告路径 （用户 > 天）	**Internet 用户**列表的旁边有一个路径，用于显示创建当前报告的选择。单击路径中的任何链接，可返回该数据的视图。
查看	选择报告的时间段：一天、一周、一月或全部。报告将更新以显示选择的时间段内的数据。 使用相邻的箭头按钮可在可用数据中移动，一次查看一个时间段 （天、周、月）。 更改此选择时，**查看范围**字段将更新以反映正在查看的时段。 如果您在 “查看范围”字段中或通过 “收藏报告”对话框选择具体日期，则**查看**字段将显示 “自定义”，而不显示时间段。
查看范围	这些字段中的日期将会自动更新，以反映您更改**查看**字段时正被查看的时间段。 或者，您可输入报告的确切开始和结束日期，或单击日历图标以选择所需日期。 然后单击相邻的右侧的箭头按钮，从而在选择日期后更新报告。
饼形图/ 条形图	条形图处于活动状态时，单击**饼形图**可以饼形图方式显示当前摘要报告。单击切片标签所显示的选项，与您单击条形图左列中项目时可用的选项相同。 饼形图处于活动状态时，单击**条形图**可以条形图方式显示当前摘要报告。
完整屏幕	选择此选项可在单独窗口中显示当前调查报告，无需左右导航窗格。

选项	操作
匿名/名称	单击**匿名**可使报告在应出现用户名的地方显示内部分配的用户标识数字。 名称隐藏时，单击**名称**可在这些位置显示用户名。 在某些情况下，用户名无法显示。更多信息，请参阅*配置 Filtering Service 以进行日志记录*，第 257 页。 如单击“匿名”，然后移到数据的不同视图（例如细节视图或异常值），则用户名在新报告中仍将保持隐藏状态。但是，要使用隐藏的名称返回摘要视图时，必须使用报告顶部的链接，而不是横幅窗格中的导航控件。 如果不应让个人管理员访问报告中的用户名，则应给他们分配相应的角色，使他们的报告权限不可查看调查报告中的用户名或访问演示报告。
搜索	从列表中选择报告元素，然后在相邻的文本框中输入部分或全部搜索值。 单击相邻的箭头按钮，可开始搜索并显示结果。 输入部分 IP 地址，例如 10.5.，则在此情况下，所有子网的搜索结果将列出从 10.5.0.0 至 10.5.255.255 的地址。

8. 通过创建多级摘要报告，可为左列中的所有或选择的项添加信息子集。请参阅*多级摘要报告*，第 104 页。
9. 通过单击相邻的数字或计量条，可为左列中的特定项目创建列表报告。此详细报告可根据您的特定需求进行修改。请参阅*灵活的详细报告*，第 105 页。

多级摘要报告

相关主题：

- *调查报告*，第 100 页
- *摘要报告*，第 101 页
- *灵活的详细报告*，第 105 页
- *用户活动详细信息报告*，第 109 页
- *标准报告*，第 113 页
- *收藏调查报告*，第 114 页
- *计划调查报告*，第 117 页
- *异常值报告*，第 119 页
- *输出到文件*，第 120 页

多级摘要报告将显示第二级信息，以补充已显示的主要信息。例如，如果主要信息显示风险级别，您可定义第二级信息，从而了解各个风险级别中被请求最多的类别。例如，如果主要报告可显示每个类别的请求，则您可显示前 5 个类别以及在每个类别中对其请求最多的前 10 名用户。

使用摘要报告正上方的设置可创建多级摘要报告。

1. 在**选择前面**列表中，选择一个数字以指定要报告的主要项（左列）数量。则结果报告将包括值最大的主要项。（如果“天”是主要项，则报告将显示最早的日期。）

   或者，勾选左列中所需单个项旁边的复选框，从而仅报告这些项。**选择前面**字段将显示**自定义**。
2. 从**按**列表中选择要报告的第二级信息。
3. 在**显示**字段中，为每个主要项选择要报告的第二级结果的数量
4. 单击**显示结果**以生成多级摘要报告。

   摘要报告将进行更新，从而仅显示选择的数量的主要项。在每个主要项条的下面，将显示第二级项的列表。
5. 使用列标题旁的箭头可更改报告的排序方式。

要返回单级摘要报告，请选择 **Internet 用户**下面的不同选项。或者，单击一个主要项或第二级项，然后选择一个选项以生成该信息的新调查报告。

灵活的详细报告

相关主题：

- *调查报告*，第 100 页
- *摘要报告*，第 101 页
- *多级摘要报告*，第 104 页
- *收藏调查报告*，第 114 页
- *计划调查报告*，第 117 页
- *异常值报告*，第 119 页
- *输出到文件*，第 120 页
- *数据库连接与报告默认*，第 280 页
- *灵活的详细报告的列*，第 107 页

详细报告可为您提供日志数据库中信息的列表视图。您可在查看摘要报告后，从主要页面访问详细报告视图以了解更多详细信息。

您可从任一行请求详细视图。但是，根据点击量请求详细报告时，建议您从小于 100,000 点击量的那一行开始。如果某特定行的点击量大于 100,000，则此点击值将显示为红色以警告您详细报告生成的速度可能会很慢。

由于详细报告视图可帮助您设计自己的报告，因此被认为具有很高的*灵活性*。您可添加或删除信息列，也可更改列的显示顺序。信息将根据列的顺序进行排序。您甚至可在任何列中反转排列顺序 （从升序到降序），反之亦然。

Websense 调查报告将受到运行 Websense Manager 的计算机的处理器、可用内存以及一些网络资源的限制。对大容量报告的请求可能会超时。请求大容量报告时，您可选择在不超时的情况下生成报告。

重要

在下拉列表或值列表中，一些选项可能会显示为红色。红字表示选择此选项可能导致容量极大的报告。通常，解决这一问题的有效方法是在选择该选项之前进一步向下搜索详细信息。

1. 在调查报告主页面上生成摘要报告或多级报告。（请参阅*摘要报告*，第 101 页或*多级摘要报告*，第 104 页。）
2. 向下搜索结果，以重点查看您所关注的信息。

   生成点击量报告时，建议您向下搜索，以查看点击量小于 100,000 的项，然后再打开细节报告视图。
3. 单击您要了解更多详细信息的行上数字或条。要在一个报告中包括多行，请勾选每一行的复选框，然后再单击该行的数字或条。

   弹出式消息将显示选项报告的加载进度。

   注意

   如果报告需要较长时间才能生成，请考虑单击 “正在加载” 消息中的链接以便将它保存为 “收藏报告”，并计划在以后运行它。请参阅*收藏调查报告*，第 114 页。
4. 查看初始报告中的信息。

   默认列将根据您的报告类型 （点击量、带宽、浏览时间以及 “选项” 页面上所作选择）不同而各异。（请参阅*数据库连接与报告默认*，第 280 页。）
5. 单击页面顶部的**修改报告**。

   “修改报告” 对话框中的**当前报告**列表可显示当前选项报告中出现的列。
6. 在**可用列**或**当前报告**列表中选择一个列名称，然后单击右侧的箭头 (>) 或左侧的箭头 (<) 按钮将该列移到其他列表。

   最多可选择报告的 7 个列。初始摘要报告中，显示衡量标准（点击量、带宽、浏览时间）的列始终位于最右边。修改报告时，它不会以选项的形式出现。

   请参阅*灵活的详细报告的列*，第 107 页，以查看可用列的列表以及每个列的描述。
7. 选择**当前报告**列表中的列名称，并使用向上和向下的箭头按钮，可更改列的顺序。

   “当前报告” 列表顶部的列将成为报告中的左列。

8. 单击报告上方的**摘要**或**细节**链接，可在两个模式之间切换。

选项	描述
摘要	要显示摘要报告，必须删除“时间”列。则摘要报告将把所有共享一个常见元素的记录合并成单一的项。根据所报告的内容不同，具体的元素也各不相同。通常，摘要元素将显示在衡量标准前面最右边的列。
细节	“细节”选项可按单独一行的方式显示每个记录，并可显示“时间”列。

9. 单击**提交**可生成您定义的报告。
10. 使用以下选项可修改显示的报告。
    - 使用报告上方的**查看**选项可更改报告的时间段。
    - 单击列标题中的向上或向下的箭头，可反转该列的排列顺序和相关数据。
    - 分别使用报告上方和下方的**下一步**和**上一步**链接，可显示报告的其他页面（如果有）。默认情况下，每个页面包含 100 行，并可根据您的需要进行调整。请参阅*显示和输出选项*，第 282 页。
    - 单击 URL 在新窗口中打开请求的网站。
11. 如果您想保存报告，请单击**收藏报告**，以便您快捷地再次或重复生成该报告（请参阅*将报告保存为“收藏报告”*，第 115 页）。

灵活的详细报告的列

相关主题：

- *灵活的详细报告*，第 105 页
- *收藏调查报告*，第 114 页
- *计划调查报告*，第 117 页

下表可用于描述详细报告的可用列（请参阅*灵活的详细报告*，第 105 页）。

并非所有列随时都可用。例如，如果显示“用户”列，则“组”不可用；如果显示“类别”，则“风险等级”不可用。

列名称	描述
用户	发出请求的用户的名称。用户信息必须在日志数据库中可用，以便将它们包括在报告之中。在基于用户的报告上，组信息不可用。
天	发出请求的日期。
URL 主机名	请求站点的域名（也称为主机名）。
域	发出请求的基于目录的客户端（用户或组、域、或是组织单位）的目录服务域。

列名称	描述
组	请求者所属的组的名称。基于组的报告中不提供单个用户名。如果请求站点的用户属于目录服务中的多个组，则报告将在此列中列出多个组。
风险级别	与请求站点所属类别相关的风险级别。如果类别属于多个风险级别，则所有相关风险级别均将列出。请参阅*指定类别的风险级别*，第 256 页。
目录对象	发出请求的用户的目录路径（用户名除外）。通常，由于每个用户都属于多个路径，这会导致相同通信出现多行。 如果您使用的是非 LDAP 目录服务，则此列不可用。
部署	Websense 软件为响应请求所作的操作，如允许的类别或阻止的类别。
源服务器	向 Filtering Service 发送请求的计算机的 IP 地址。该计算机可运行集成产品或 Websense Network Agent。
协议	请求的协议。
协议组	请求协议所属的主数据库组。
源 IP	发出请求的计算机的 IP 地址。
目标 IP	请求站点的 IP 地址。
完整 URL	请求站点的域名和路径（例如：http://www.mydomain.com/products/itemone/）。如果您未记录完整 URL，则此列为空。请参阅*配置完整 URL 记录*，第 273 页。
月	发出请求的日历月。
端口	用户与站点通讯的 TCP/IP 端口。
带宽	包括在用户的初始请求和网站的响应中包括的所有数据量（以 KB 为单位），是发送值和接收值的总和。 请记住，某些集成产品不向 Websense 软件发送信息，例如 Check Point FireWall-1 和 Cisco PIX Firewall。如果您的集成产品不发送此信息，且 Websense Network Agent 已安装，请激活相应 NIC 的**记录 HTTP 请求**选项以启用带宽信息报告。请参阅*配置 NIC 设置*，第 292 页。
已发送字节	Internet 请求发送的字节数。此数字代表已传输的数据量，它可以是简单的 URL 请求，或是在用户注册网站时提交的重要内容。

列名称	描述
已接收字节	相应请求时从 Internet 接收的字节数。其中包括构成站点的所有文本、图形和脚本。 对于已阻止的站点而言，字节数根据创建日志记录的软件不同而各异。当 Websense Network Agent 进行记录时，已阻止站点所接收的字节数代表阻止页面的大小。 如果日志记录由 Websense Security Gateway 创建，则作为实时扫描的结果，收到的字节数将代表已扫描页面的大小。请参阅*分析带实时选项的内容*，第 123 页，以了解更多有关实时扫描的信息。 如果由其他集成产品创建日志记录，则已阻止站点所接收的字节可能为零（0），可能代表阻止页面的大小，也可能是从请求的站点获得的值。
时间	站点收到请求当天的时间，显示格式为 HH:MM:SS（采用 24 小时制）。
类别	筛选请求的类别。该类别可能是 Websense 主数据库中的类别，或是自定义类别。

用户活动详细信息报告

相关主题：

- *调查报告*，第 100 页

单击**用户每日/月**链接可生成某个用户的“用户活动详细信息”报告。此报告将为一天或一整个月中的用户 Internet 活动提供图解说明。

首先，生成特定用户在选定的一天中的报告。您可从此报告生成该用户在一整个月内的活动报告。有关详细信息，请参阅：

- *用户每日活动详细信息*，第 109 页
- *用户每月活动详细信息*，第 111 页

用户每日活动详细信息

相关主题：

- *调查报告*，第 100 页
- *用户活动详细信息报告*，第 109 页
- *用户每月活动详细信息*，第 111 页

用户每日活动详细信息报告可帮助您更深入地查看指定用户在某一天的活动。

1. 选择主页面顶部的**用户每日/月**将出现“用户每日活动详细信息”对话框。

2. 在**搜索用户**字段中输入用户名或部分名称，然后单击**搜索**。

   搜索结果将显示一个滚动列表，其中可含最多 100 个日志数据库中的匹配用户名。

3. 在**选择用户**列表中进行选择。

4. 在**选择日期**字段中，您可接受默认显示的上一个活动日期，或者选择其他日期。

   您可键入新日期，或单击日历图标以选择日期。日历选择方框显将指明活动的日志数据库所涵盖的日期范围。

5. 单击**按天查看用户**可查看该用户在请求日期的活动的详细报告。

   初始报告将以每次增加 5 分钟的方式显示用户活动的时间线。每个请求将以图标形式显示，与 Websense 主数据库类别相对应。单一图标可代表所有的自定义类别。（图标颜色与 “用户每月活动”报告中显示的风险分组相对应。请参阅*用户每月活动详细信息*，第 111 页。）

   将鼠标置于图标上可显示相关请求的确切时间、类别和操作。

   使用下方列出的控件可修改报告显示或查看图例。

选项	描述
上一日 / 下一日	显示该用户在上一个日历日或下一个日历日的 Internet 活动。
表格视图	显示每个请求的 URL 列表，提供请求的日期和时间、类别以及采取的操作 （阻止、允许或其他）等信息。
详细视图	显示报告的初始图形视图。
群组类似点击 /查看所有点击量	将所有在 10 秒钟内发生的，并具有相同域、类别和操作的请求合并到单一行。这样可生成更为简短的信息摘要视图。 标准时间阈值为 10 秒。如果您需要更改此值，请参阅*显示和输出选项*，第 282 页。 单击此链接后，它将变成 “查看所有点击量”，可用于恢复每个请求的初始列表。
类别视图控制	显示当前报告中每个类别的列表，为您提供类别名称和代表该类别的图标。 通过勾选要包括的类别的复选框，可控制报告中将显示的类别。然后单击**接受**以根据您的选择更新报告。

6. 单击报告上方的**用户每月活动详细信息**可查看同一用户一整个月中的活动。请参阅*用户每月活动详细信息*，第 111 页，以了解更多信息。

用户每月活动详细信息

相关主题：

- *调查报告*，第 100 页
- *用户活动详细信息报告*，第 109 页
- *用户每日活动详细信息*，第 109 页
- *类别地图*，第 111 页

“用户每日活动详细信息”报告打开时，您可切换以查看该用户的每月活动。

1. 打开“用户每日活动详细信息”报告。请参阅*用户每日活动详细信息*，第 109 页。
2. 单击顶部的**用户每月活动详细信息**。

   新报告将显示日历图像，其中每一天区域中的一些细小的彩色方块，可代表用户在该日的 Internet 活动。自定义类别中的站点请求将显示为灰色方块。
3. 单击左上方的**数据库类别图例**可查看代表请求网站潜在风险从低到高的不同颜色。

   类别分配是固定的，且不能更改。请参阅*类别地图*，第 111 页。
4. 单击**上一个**或**下一个**可显示用户在上一个月或下一个月的 Internet 活动。

类别地图

相关主题：

- *调查报告*，第 100 页
- *用户活动详细信息报告*，第 109 页
- *用户每月活动详细信息*，第 111 页

以下列表可指明“用户每日活动”报告和“用户每月活动详细信息”报告上每种颜色代表的相应类别。

请记住，主数据库中的类别名称可能会更改。而且，类别可随时添加或删除。

颜色	类别
灰色	自定义类别 非 HTTP 通信
深蓝色	**商业与经济**及其所有子类别 **教育**及其所有子类别 **健康** **信息技术**（包括搜索引擎和门户）及网络托管子类别 **其他**子类别，如内容发送网络、动态内容、图像（媒体）、图像服务器和私有 IP 地址 **生产力**/广告
浅蓝色	**药物**/处方药 **政府**及其军事子类别 **信息技术**/URL 翻译站点 **其他**，仅限父类别 **新闻与媒体**，仅限父类别 **特殊活动**
黄色 绿色	**堕胎**及其所有子类别 **成人资料**/性教育 **带宽**，包括 Internet 广播与电视、个人网络存储与备份和流媒体子类别 **娱乐**，包括其 MP3 子类别 **游戏** **政府**/政治机构 **信息技术**/计算机安全 **Internet 通讯**/基于 Web 的电子邮件 **其他**/文件下载服务器 **其他**/网络错误 **新闻与媒体**/替代性期刊 **生产力**，包括即时消息、留言板和论坛、在线经纪人代理和交易子类别 **宗教**及非传统宗教和神秘学以及民俗和传统宗教子类别 **安全**，仅限父类别 **购物**及其所有子类别 **社会机构**及其所有子类别 **社会和生活方式**，包括同性恋与双性恋兴趣、爱好、个人网站、餐厅与餐饮子类别 **体育**及其所有子类别 **旅行** **用户定义** **汽车**

颜色	类别
橙色	**成人资料**/裸体 **倡导组织** **带宽**/Internet 电话 **药物**及滥用药物、大麻、补充药物和未规范化合物子类别 **信息技术**/代理规避 **Internet 通讯**及网络聊天子类别 **工作搜索** **其他**/未分类 **生产力**子类别，如免费软件和软件下载以及冲浪赚钱 **宗教** **社会和生活方式**子类别，如酒精与烟草、个人生活与约会 **品味低下** **武器**
红色	**成人资料**及子类别 成人内容、内衣、泳装和性 **带宽**/对等文件共享 **赌博** **非法或可疑** **信息技术**/黑客 **军事与极端主义** **种族主义与仇恨** **安全**子类别，如键盘记录程序、恶意网站、网络钓鱼和间谍软件 **暴力**

标准报告

相关主题：

- *调查报告*，第 100 页
- *收藏调查报告*，第 114 页
- *计划调查报告*，第 117 页

标准报告可帮助您无需向下搜索即可快速显示特定的信息组。

1. 单击“调查报告”主页面上的**标准报告**链接。

2. 选择包含所需信息的报告。则可提供以下报告。

最高活动级别
• 哪些用户有最多的点击量？ • 访问次数最多的前 10 个 URL 的前 10 名用户 • 购物、娱乐和体育活动最多的前 5 名用户 • 访问次数最多的前 5 个类别的前 5 个 URL
最高带宽消耗
• 哪些群组消费最多的带宽 • 消耗流媒体中带宽最多的群组 • 有关用户网络带宽损失的详细 URL 报告 • 前 10 个带宽类别组
最常在线
• 哪些用户最常在线 • 哪些用户在生产力类别中的站点上花费的时间最多
最常被阻止的
• 哪些用户最常被阻止？ • 哪些站点最常被阻止？ • 有关被阻止用户的详细 URL 报告 • 10 个最常被阻止的类别
最高安全风险
• 造成安全风险的主要类别 • P2P 协议的前几个用户 • 安全类别中的前几个站点用户 • 前 10 台最常有间谍软件活动的计算机的 URL
法律责任
• 按类别的法律责任风险 • 成人类别中的前几个用户

3. 查看显示的报告。
4. 如果您想重复运行报告，请将它保存为“收藏报告”。请参阅*收藏调查报告*，第 114 页。

收藏调查报告

相关主题：

- *调查报告*，第 100 页
- *计划调查报告*，第 117 页

您可将大部分调查报告保存为**收藏报告**，其中包括向下搜索具体信息时生成的报告、标准报告以及根据您具体需求修改的详细报告。然后您可随时运行 “收藏报告”，也可将其计划为在具体日期或时间运行。

在使用委派管理的组织中，由超级管理员可设置保存和计划 “收藏报告” 的权限。获此权限的管理员只能运行和计划他们自己保存的 “收藏报告”，不得访问其他管理员保存的 “收藏报告”。

有关使用 “收藏报告” 的详细说明，请参阅：

- *将报告保存为 “收藏报告”，第 115 页*
- *生成或删除 “收藏报告”，第 115 页*
- *修改 “收藏报告”，第 116 页*

将报告保存为 “收藏报告”

相关主题：

- *收藏调查报告，第 114 页*
- *修改 “收藏报告”，第 116 页*

使用以下步骤可将报告保存为收藏报告。

1. 使用所需格式和信息生成调查报告。
2. 单击**收藏报告**。
3. 接受或修改 Websense Manager 显示的名称。

   此名称可包含字母、数字和下划线字符 (_)，不得包含空格或其他特殊字符。
4. 单击**添加**。

   则报告名被添加到 “收藏报告” 列表。
5. 选择列表上的报告，然后选择管理报告的选项。根据您选择的选项，请参阅：
   - *生成或删除 “收藏报告”，第 115 页*
   - *计划调查报告，第 117 页*

生成或删除 “收藏报告”

相关主题：

- *收藏调查报告，第 114 页*
- *修改 “收藏报告”，第 116 页*

您可随时生成收藏报告，或删除已过时的报告。

1. 单击**收藏报告**可显示保存为 “收藏报告” 的报告列表。

   注意
   如果您的组织使用委派管理，则此列表将不包括其他管理员保存的收藏报告。

2. 从列表中选择所需报告。

   如果所需报告还未保存为“收藏报告”，请参阅*将报告保存为“收藏报告”*，第 115 页。

3. 根据您的需要：
   - 单击**立即运行**以立即生成并显示选择的报告。
   - 单击**计划**可将报告计划为在以后运行或重复运行。请参阅*计划调查报告*，第 117 页，以了解更多信息。
   - 单击**删除**可从 “收藏报告” 列表中删除报告。

修改 “收藏报告”

相关主题：
- *调查报告*，第 100 页
- *收藏调查报告*，第 114 页

您可用以下方式轻松创建类似于现有 “收藏报告 “的新收藏报告：

1. 单击**收藏报告**可显示保存为 “收藏报告” 的报告列表。

   注意
   如果您的组织使用委派管理，则此列表将不包括其他管理员保存的收藏报告。

2. 选择并运行与您要创建的新报告最为类似的现有 “收藏报告”。（请参阅*生成或删除 “收藏报告”*，第 115 页。）
3. 根据需要修改显示的报告。
4. 单击**收藏报告**可使用新名称将已修改的报告保存为 “收藏报告”。（请参阅*将报告保存为 “收藏报告”*，第 115 页。）

计划调查报告

相关主题：

- *收藏调查报告*，第 114 页
- *将报告保存为 “收藏报告”*，第 115 页
- *管理计划的调查报告作业*，第 119 页

您必须将调查报告保存为 “收藏报告” 后才能将其计划为在以后运行或重复循环运行。计划的报告作业运行时，结果报告将通过电子邮件发送给您指定的收件人。创建计划作业时，请考虑您的电子邮件服务器是否能够处理所附报告文件的大小和数量。

计划的报告文件将存储在以下目录：

```
< 安装路径 >\webroot\Explorer\< 名称 >\
```

默认安装路径为 C:\Program Files\Websense。如果计划作业只有一个收件人，则 <名称>是电子邮件地址的第一部分 （@ 前面的内容）。如果有多个收件人，则报告将保存在名为 Other 的目录中。

注意

通过重复作业保存的报告每次都会使用相同的文件名。如果您想保存文件的时间要长于一次循环的时间，请务必更改文件名或将文件复制到其他位置。

根据所计划报告的大小和数量，目录可能会非常大。请确保定期清除目录，以删除不必要的报告文件。

1. 将一个或多个报告保存为 “收藏报告” 。（请参阅*将报告保存为 “收藏报告”*，第 115 页）。
2. 单击**收藏报告**可显示保存为 “收藏报告” 的报告列表。

   注意

   如果您的组织使用委派管理角色，则此列表将不包括其他管理员保存的收藏报告。

3. 最多可突出显示 5 个报告，使其作为作业的一部分而运行。
4. 单击**计划**可创建计划的报告作业，并提供 “计划报告” 页面上请求的信息。

建议您在不同日期或不同时间计划报告作业，以避免因日志数据库负荷过大而导致降低记录和互动报告的性能。

字段	描述
递归	选择运行报告作业的频率（一次、每日、每周、每月）。
开始日期	选择第一次（或唯一一次）运行作业的日期（一周中的星期几或日历日期）。
运行时间	设置运行作业当天的时间。
电子邮件发送到	使用**其它电子邮件地址**字段可将相应地址添加到此列表。 突出显示一个或多个电子邮件地址，以接收作业中的报告。（请确保取消选中不应接收报告的地址。）
其它电子邮件地址	输入电子邮件地址，然后单击**添加**将它放入**电子邮件发送到**列表。 系统将自动突出显示新电子邮件地址将和其他选择的电子邮件地址。
自定义电子邮件主题和正文文本	勾选此复选框可自定义您的电子邮件通知主题行和正文文本。 如果此框未被选中，则将使用默认主题和正文文本。
电子邮件主题	输入文本以作为分发计划的报告时显示的电子邮件主题行。 默认的电子邮件主题为： 调查报告计划作业
电子邮件文本	输入要添加到用于分发计划的报告的电子邮件消息中的文本。 电子邮件内容如下所示，用您的文本将代替 <CUSTOM TEXT>。 由 Report scheduler 生成的附加文件或 < 日期时间 > 文件。 <CUSTOM TEXT> 单击以下链接可查看生成的报告。 注意：如果接收者无法访问发送作业的网络服务器，链接将无法使用。
计划作业名称	为计划作业分配唯一的名称。该名称可用于在“作业队列”中识别此作业。请参阅 *管理计划的调查报告作业*，第 119 页。
输出格式	选择计划的报告的文件格式。 **PDF**：便携式文档格式文件需在 Adobe Reader 中查看。 **Excel**：Excel 电子表格文件需在 Microsoft Excel 中查看。
日期范围	设置此作业中报告涵盖的日期范围。 **所有日期**：日志数据库中的所有可用日期。 **相对**：选择要包括的时间段（“天”、“周”或“月”）和特定的时间段（“本时间段”、“最近 1 个时间段”、“最近 2 个时间段”等等）。 **特定**：设置此作业中报告的具体日期或日期范围。

5. 单击**下一步**显示 “计划确认” 页面。
6. 单击**保存**以保存您的选择并转至 “作业队列” 页面 （请参阅 *管理计划的调查报告作业*，第 119 页）。

管理计划的调查报告作业

相关主题：

- *调查报告*，第 100 页
- *计划演示报告*，第 94 页

创建调查报告的计划作业时，将出现**作业队列**页面，可显示新作业和现有计划作业列表。您也可通过单击调查报告主页面上的**作业队列**链接访问此页面。

注意

如果您的组织使用委派管理，则此页面将不显示其他管理员计划的作业。

计划报告细节部分将按创建时的顺序列出每个计划作业，并提供已定义计划和作业状态的概述。此外，还提供以下选项。

选项	描述
编辑	显示针对此作业定义的计划，并可根据需要对其进行修改。
删除	删除作业并在 “状态日志” 部分中添加项，使该作业显示为 “已删除”。

状态日志部分将列出每项已更改的作业，显示该作业的计划开始时间、实际结束时间和状态。

单击**清除状态日志**可删除 “状态日志” 部分中的所有项。

异常值报告

相关主题：

- *调查报告*，第 100 页
- *摘要报告*，第 101 页

异常值报告可显示数据库中 Internet 活动最为异常的用户。 Websense 软件将根据每个类别、每天、每个操作 （有时称为部署）和每个协议计算所有用户的平均活动，然后显示在统计上与平均值相比变化最大的的用户活动。此变化将按与平均值比较的标准偏差来计算。

1. 在调查报告主页面可生成摘要报告，其中显示了与您查看异常值的原因相关的信息。“Internet 用户”字段旁加下划线并显示为蓝色的报告选择将反映在 “异常值”报告中。

   例如，要查看特定类别的点击量异常值，请选择 **Internet 用户**列表中的**类别**，然后选择**点击量**作为**衡量标准**。

   > **注意**
   > 软件无法根据浏览时间生成异常值报告。如果您以显示浏览时间的摘要报告开始，则 “异常值”报告只可根据点击量而生成。

2. 单击**异常值**。

   所有行将以降序方式排列，具有最高变化值的行将显示在最前面。每一行将显示：

   - 用户、类别、协议、天和操作的总量 （点击量或带宽）。
   - 所有用户、类别、协议、天和操作的平均值 （点击量或带宽）。
   - 用户偏离于平均值的变化。

3. 要查看单个用户在此类别中随时间而变化的活动，请单击用户名。

   例如，如果一个用户的活动在某一天异常频繁，请单击该用户的名称以查看报告，从而深入了解该用户的总体活动。

输出到文件

相关主题：

- *调查报告*，第 100 页
- *打印调查报告*，第 121 页

生成调查报告后，您可使用报告上方的按钮将报告保存到文件。您所单击的按钮将决定文件的格式。

选项	描述
	以 XLS 格式保存报告。 如果用于访问 Websense Manager 的计算机上安装了 Microsoft Excel 2003 或更高版本，则系统将提示您查看或保存报告。否则，系统将提示您为保存的报告选择目录和文件名。 Microsoft Excel 中的选项可用于打印、保存或通过电子邮件发送报告。
	以 PDF 格式生成报告。 如果用于访问 Websense Manager 的计算机上安装了 Adobe Reader v7.0 或更高版本，则系统将提示您查看或保存报告。否则，系统将提示您为保存的报告选择目录和文件名。 Adobe Reader 中的选项可用于打印、保存或通过电子邮件发送报告。

打印调查报告

相关主题：

- *调查报告*，第 100 页
- *输出到文件*，第 120 页

您可用以下方式打印调查报告：

- 显示报告时使用 Web 浏览器的打印功能。
- 创建 PDF 或 XLS 文件，然后使用 Adobe Reader 或 Microsoft Excel 中的打印功能（请参阅*输出到文件*，第 120 页）。

尽管报告已被设置为可从浏览器成功打印，但您可能需要测试打印以检查结果。

“用户每月活动详细信息”报告被配置为以横向模式打印，其他所有报告则被配置为纵向模式。

设计您自己的报告时（请参阅*灵活的详细报告*，第 105 页），列宽应按照所包括的信息而有所不同。如果报告宽度大于 8.5 英寸，页面方向将更改为横向。

页面内容宽度为 7 1/2 英寸或 10 英寸。如果使用 A4 纸打印，页边距会较窄，但仍在打印范围之内。（默认的纸张规格为 Letter 或 8.5 x 11 英寸。如使用 A4 纸，请务必更改 wse.ini 文件中的此项设置。请参阅*显示和输出选项*，第 282 页。）

访问自我报告

相关主题：

- *调查报告*，第 100 页
- *配置报告首选项*，第 257 页
- *自我报告*，第 284 页

Websense 自我报告可使您评估自己的 Internet 浏览活动并根据需要进行调整，以符合组织的方针。若政府规定组织应允许用户可查看正在收集的信息类型，它也可满足这一要求。

如果在您的组织中启用了自我报告，请从您的浏览器对其进行访问。

1. 输入 Websense 管理员提供的 URL，或单击主 Websense Manager 登录页面上的“自我报告”链接以访问自我报告登录页面。
2. 如果 **Policy Server** 显示下拉菜单，请选择记录 Internet 活动信息的 Policy Server 的 IP 地址。

   请与您的 Websense 管理员联系以获得帮助。

3. 输入您登录网络时使用的**用户名**和**密码**。
4. 单击**登录**。

Websense Manager 将打开一份调查报告，并按风险级别显示您的 Internet 活动。单击页面上的不同链接和元素可访问其他选项，以获得存储在您活动上的信息的其他视图。操作报告时，可使用**帮助**系统以获得帮助。

7 分析带实时选项的内容

相关主题：

- *扫描选项*，第 124 页
- *进行内容分类并扫描威胁*，第 125 页
- *文件扫描*，第 126 页
- *去除内容*，第 127 页
- *实时扫描活动报告*，第 130 页

Websense 筛选软件将以您的活动策略和存储于主数据库中的信息为基础对 Internet 活动进行筛选。如果您订购了 Websense Content Gateway 或 Websense Web Security Gateway，您也可以对网站和文件内容进行实时分析。

根据您的订购，有 2 项实时分析选项可供使用：内容分类和安全实时扫描。

- 使用**内容分类**可查看未被阻止的 URL 内容（基于您的活动策略和 URL 的 Websense 主数据库分类），并返回可供筛选使用的类别。
- 如果您订购了 Websense Web Security Gateway，则有 3 项**安全实时扫描**选项可供使用。
  - **内容扫描**可查看网络内容以查找安全威胁，如网络钓鱼、URL 跳转、网络漏洞攻击病毒，以及代理避免。
  - **文件扫描**可探测文件内容，以决定威胁类别，如病毒、木马、或蠕虫。
  - **内容去除**可从请求的网页中删除活动的内容。

以上选项被激活后，只有那些根据您的活动策略和站点的 Websense 主数据库类别**未**被阻止的站点会被加以分析。更多信息，请参阅*扫描选项*，第 124 页。

重要

受限访问筛选器和未筛选的 URL 优先于实时分类。

如果用户请求激活的“受限访问筛选器”（请参阅*限制用户只能访问已定义列表中的 Internet 站点*，第 141 页）中或“未筛选的 URL”列表（请参阅*针对特定站点重新定义筛选*，第 153 页）中的一个站点，则即使已启用实时扫描并已发现威胁，该请求仍将被允许。

要利用这些实时安全功能，请在以下两处输入可支持 Websense Content Gateway 或 Websense Web Security Gateway 的订购密钥:

- 在 Websense Manager 中 （请转至**设置 > 帐户**）。
- 在 Websense Content Gateway 管理界面（请转至**配置 > 我的代理 > 订购 > 订购管理**选项卡）。

这 2 个产品需花费数分钟时间下载必要的数据库、同步软件，并显示这两个管理工具中所有的实时功能。

Websense 实时选项

Websense 实时选项可帮助确保网络的安全性。使用这些选项可对 Internet 内容进行扫描并将其分配到一个筛选类别。实时结果将被发送至 Filtering Service，后者将根据活动策略中分配至其实时分类的操作对站点进行筛选。

数据库下载

实时选项将依赖于和 Websense Web Security Gateway 一起安装的小型数据库，Websense Web Security Gateway 将按固定间隔时间检查数据库更新。这些数据库的更新与所有主数据库更新（包括实时数据库更新和实时安全更新）均无关联。

每次使用 **./WCGAdmin start** 命令来启动 Websense Security Gateway 时，数据库下载即被启动。如果下载失败，则会每 15 分钟重新尝试新的下载，直至下载成功为止。

默认的数据库更新检查间隔为 15 分钟。您可在 Websense Content Gateway 计算机上的 **/opt/bin/downloadservice.ini** 文件中，通过编辑 **PollInterval** 值来更改此时间间隔。

编辑 **downloadservice.ini** 文件后，您必须通过命令行停止并重新启动 Websense Content Gateway。

- 要停止，请输入：**/opt/WCG/WCGAdmin stop**
- 要重新启动，请输入：**/opt/WCG/WCGAdmin start**

扫描选项

使用**设置 > 实时扫描**页面可启用并配置实时选项。在以下部分中我们将对单个扫描选项进行详细介绍。

- *进行内容分类并扫描威胁*，第 125 页
- *文件扫描*，第 126 页
- *去除内容*，第 127 页

每个选项至少有 2 个选择：

- **关闭**无实时扫描或阻止发生。该选项不会提供额外的安全性。
- **推荐**或**打开**。如果您的站点被配置为进行实时扫描，则此设置将为您提供最佳性能。扫描的执行将基于 2 个因素：
  - **设置 > 实时扫描 > 例外**选项卡上的 “总是扫描”和 “永不扫描”列表（请参阅*改善扫描*，第 128 页）。
  - 无论 Websense 软件是否将站点识别为包含动态内容，被标记为含有动态内容的站点都将被扫描。用户无法对将站点识别为含有动态内容的标记进行配置。

    含有 “永不扫描”列表中所显示动态内容的站点将不会被扫描。
- **所有**。所有被请求的网页都将被扫描。只有列于 “永不扫描”列表中的网页将不会被扫描。

  该选项提供的安全性最高，但会明显降低系统的运行速度。

警告

“永不扫描”列表中的站点在任何环境下都不会被分析。如果 “永不扫描”列表中的站点受到威胁，实时选项将无法分析并检测到恶意代码。

进行内容分类并扫描威胁

相关主题：

- *扫描选项*，第 124 页
- *文件扫描*，第 126 页
- *去除内容*，第 127 页
- *改善扫描*，第 128 页
- *实时扫描活动报告*，第 130 页

Web 内容的变化非常迅速。统计信息表明，绝大多数的 Web 内容均属于动态内容。此外，Internet 上还承载着更多由用户生成的内容，例如社交网站上的一些内容。本材料不受管理公司网站的内容和风格指南所限制。

启用内容分类之后，选定的站点将进行实时分类，而且其类别结果将被转发至 Websense 筛选软件，根据活动策略被判断应被阻止或是允许。

重要

如果您计划生成实时扫描活动报告，请启用完整 URL 记录（请参阅*配置完整 URL 记录*，第 273 页）。否则，日志记录将仅包含已分类站点的域 (www.domain.com)，而且一个站点内的各个页面可能会被分类至不同类别。

如果您的站点使用 WebCatcher 来向 Websense, Inc. 报告未分类 URL （请参阅*配置 WebCatcher*，第 267 页），则通过内容分类的 URL 将被转发加入主数据库中。

如果您的订购包含了 Websense Security Gateway，您也可以指定需扫描的站点以检测安全威胁。

使用**设置 > 实时扫描 > 常用选项**页面可指定使用内容分类和内容扫描的时间。

1. 在 “内容分类” 区域，选择**关闭**或**打开** （默认）以确定是否执行扫描。请参阅*扫描选项*，第 124 页。

   类别确定之后，您所配置的任何其他实时选项将被应用以提供额外的安全性。
2. (*Websense Security Gateway*) 在 “内容扫描” 区域，选择**关闭** （默认）、**推荐**或**所有**以确定扫描级别。
3. 进行下列操作之一：
   - 要将站点添加至 “永不扫描” 或 “总是扫描” 列表，请选择**例外**选项卡。请参阅*改善扫描*，第 128 页。
   - 要更改其他实时选项的设置，请在**常用选项**页面继续操作。请参阅*文件扫描*，第 126 页和*去除内容*，第 127 页。
4. 在完成后，请单击**确定**以缓存您的更改。直到您单击**全部保存**之后，更改才会生效实施。

演示报告可提供与对威胁网站的访问尝试有关的详细信息。请参阅*演示报告*，第 84 页，以获得有关运行 Websense 报告的详细信息。

文件扫描

相关主题：

- *扫描选项*，第 124 页
- *进行内容分类并扫描威胁*，第 125 页
- *去除内容*，第 127 页
- *改善扫描*，第 128 页
- *实时扫描活动报告*，第 130 页

文件扫描可查看用户尝试下载或远程打开的传入应用程序文件中的内容。此实时选项将向 Websense 筛选软件返回一个类别，从而在恰当情况下允许或阻止该文件。

最佳措施是扫描所有**可执行**文件（例如，**.exe** 和 **.dll** 文件）。您也可确定更多需要扫描的文件类型，并为要扫描的文件大小设定最大值。

注意

只有 Windows 32 位的便携软件文件才会被扫描。

使用**设置 > 实时扫描 > 常用选项**选项卡可指定使用文件扫描的时间。

1. 在“文件扫描”区域，选择**关闭**、**推荐**（默认）或**所有**以确定扫描级别。请参阅*扫描选项*，第 124 页。
2. 单击**高级设置**。
3. **扫描具有可执行内容的所有类型的文件**将是默认选择。如果您希望列出要扫描的单个文件扩展名，请取消选中该复选框。
4. 要指定需扫描的其他文件类型，请输入文件扩展名（例如 **ppt** 或 **wmv**），然后单击**添加**。文件扩展名只可包含字母或数字字符、下划线 (_) 或连接线 (-)。请勿在扩展名前输入圆点。

   要从指定的文件扩展名列表中删除一个文件扩展名，请选中该扩展名，然后单击**删除**。
5. 在选项中，输入需扫描文件的最大大小（默认情况下该值为 10 MB）。选择**自定义**可输入最多 4096 MB (4 GB) 的文件大小值。大于指定大小的文件将不会被扫描。
6. 进行下列操作之一：
   - 如果您想将站点添加至“永不扫描”或“总是扫描”列表，请选择**例外**选项卡。请参阅*改善扫描*，第 128 页。
   - 如果您想更改其他实时选项的设置，请在**常用选项**选项卡继续操作。请参阅*进行内容分类并扫描威胁*，第 125 页和*去除内容*，第 127 页。
7. 在完成后，请单击**确定**以缓存您的更改。直到您单击**全部保存**之后，更改才会生效实施。

演示报告将提供有关对包含安全风险文件的下载尝试的详细信息。请参阅*演示报告*，第 84 页，以获得有关运行 Websense 报告的说明。

请参阅*根据文件类型管理通信*，第 163 页，以获得有关根据类型和 URL 类别阻止文件的信息。

去除内容

相关主题：

- *扫描选项*，第 124 页
- *进行内容分类并扫描威胁*，第 125 页
- *文件扫描*，第 126 页
- *改善扫描*，第 128 页
- *实时扫描活动报告*，第 130 页

针对您的系统的威胁可隐藏在通过网页发送的活动内容中。保护您的系统完整性的一个方法是确保永不接收此类内容。

Websense 实时选项使得从传入网页中指定需去除的特定脚本语言 （ActiveX、JavaScript 或 VB Script）内容成为可能。如果启用内容去除，则所有特定去除语言中的内容将从标记为包含动态内容的站点或 “总是扫描” 类别中显示的站点中被删除 （请参阅*扫描选项*，第 124 页）。

只有在实时选项已将文件分类且 Websense 筛选软件已确定应用何种策略之后，内容才会被删除。

> **重要**
> 依赖于被删除活动内容的网页将无法按预期正常工作。要允许对需要活动内容的站点的完整访问，请禁用内容去除功能或将站点添加至 “永不扫描” 列表。

请求带有活动内容的网页的用户，将不会收到任何提示内容已被删除的通知。

使用**设置 > 实时扫描 > 常用选项**选项卡可指定从带有动态内容的站点中去除内容的时间。

1. 在 “内容去除” 区域，选择需从传入网页中删除的活动内容的类型。
2. 要更改其他实时选项的设置，请参阅：
   - *进行内容分类并扫描威胁*，第 125 页
   - *文件扫描*，第 126 页
3. 在完成后，请单击**确定**以缓存您的更改。直到您单击**全部保存**之后，更改才会生效实施。

要禁用对任何指定语言内容的去除，请取消选中相关的复选框。

改善扫描

相关主题：

- *扫描选项*，第 124 页
- *进行内容分类并扫描威胁*，第 125 页
- *文件扫描*，第 126 页
- *去除内容*，第 127 页

使用 “总是扫描” 和 “永不扫描” 列表可自定义 “推荐” 和 “所有” 扫描选项的操作。

- 当实时选项被设定为 “推荐” 或 “打开” 时，带有动态内容的站点和 “总是扫描” 列表中的站点将被扫描 （请参阅*扫描选项*，第 124 页）。而 “永不扫描” 列表中的站点将被忽略。

- 当实时选项被设定为 “所有” 时，“永不扫描” 列表中的站点将被忽略。这将提高系统的性能。

请谨慎使用 “永不扫描” 列表。如果此列表中的站点受到威胁，Websense Security Gateway 将无法对此站点进行扫描以找出其中的安全问题。

使用**设置 > 实时扫描 > 例外**页面可填充并编辑 “总是扫描” 和 “永不扫描” 列表。

要添加站点至 “总是扫描” 或 “永不扫描” 列表：

1. 请在 **URL** 框中输入站点名称。

   仅输入主机名称 （例如， **thissite.com**）即可，不必输入完整 URL。请确保输入域和扩展名； **thissite.com** 和 **thissite.net** 是不同的项。

   您可一次输入多个主机名称。
2. 在**选项**列中，选择将应用于您所输入的所有站点的实时选项。您可选择一个或多个选项。请注意，**安全威胁**仅涉及内容扫描，而非文件扫描。文件扫描不会受 “总是扫描” 和 “永不扫描” 列表影响。

   要对不同站点应用不同选项，请分别输入站点。
3. 选择**添加到 “总是扫描”** 或**添加到 “永不扫描”**。

   一个站点只可显示于这 2 个列表之一。例如，您无法指定同一个站点既要总是接受扫描以发现威胁，又永不接受内容去除。

   - 要更改一个站点所属的列表，首先选中该站点，然后使用右箭头 (>) 和左箭头 (>) 按钮将其移动至新列表中。
   - 要从列表中删除一个站点，请选中该站点，然后单击**删除**。
4. 在完成后，请单击**确定**以缓存您的更改。直到您单击**全部保存**之后，更改才会生效实施。

要更改与站点相关的扫描选项：

1. 在 “总是扫描” 或 “永不扫描” 列表中选择该站点，然后单击**编辑**。
2. 在 “编辑规则” 框中，为该站点主机名称选择新选项：
   - 选择**不更改**将保持当前设置。
   - 选择**打开**则表明内容将按指定选项 （例如内容分类）进行扫描。
   - 选择**关闭**则表明对指定选项不作任何扫描。如果选项关闭，性能将得到提高，但安全性将受到危害。
3. 完成更改之后，请单击 “编辑规则” 框中的**确定**返回 “例外” 选项卡。
4. 再次单击**确定**以缓存您的更改。直到您单击**全部保存**之后，更改才会生效实施。

实时扫描活动报告

相关主题：

- *扫描选项*，第 124 页
- *进行内容分类并扫描威胁*，第 125 页
- *文件扫描*，第 126 页
- *去除内容*，第 127 页

如果您的订购包含实时扫描功能，您可使用演示报告和调查报告对这些功能的效果进行分析。

在“演示报告”页面可查看一组名为“实时安全威胁”的报告。这些报告主要用于专门记录与威胁相关的活动。利用所有演示报告，您可复制安全威胁报告并编辑它的报告筛选器，从而在您从这个副本生成报告时对其中包含的信息进行提炼。

有些安全威胁报告中包含一个“威胁 ID”列。您可单击单个威胁 ID 以打开 Websense Security Labs 页面，其中将描述被识别的威胁的类型。

此外，其他演示报告还包含实时扫描活动以及标准筛选活动的相关信息。复制预定义报告并编辑其筛选器可创建一份特定的实时扫描活动报告。

重要

启用完整 URL 记录（请参阅*配置完整 URL 记录*，第 273 页）将确保实时扫描活动报告内容详尽有效。否则，即使站点内的单个页面被分至不同类别或包含不同威胁，报告也仅会显示已分类站点的域 (www.domain.com)。

例如，在报告编录的“Internet 活动”组中可找到“类别的完整 URL 详细信息”报告，其中提供了各个类别中被访问的每个 URL 的详细列表。要制作实时扫描报告，请复制“类别的完整 URL 详细信息”报告并编辑其报告筛选器。在“操作”选项卡上，仅选择与实时扫描相关的允许或阻止操作。在“选项”选项卡上，更改报告编录标题和报告名称以便将此报告识别为实时扫描报告。例如，您可将名称和标题更改为《实时：类别的完整 URL 详细信息》。

调查报告也可用于了解实时扫描活动的进程。

1. 在 **Internet 用户**下拉列表中选择“操作”。
2. 在结果报告中单击一个实时操作（例如实时阻止的类别）将显示一个交互式选项的列表。
3. 单击想要的交互式选项，例如“类别”或“用户”。
4. 单击任何行上的“点击量”值或条可查看相关详细信息。
5. 在页面顶部单击**修改报告**可在报告中添加完整 URL 列。

   请参阅*调查报告*，第 100 页，以了解使用所有调查报告功能的详细信息。

如何记录实时扫描

当您使用实时扫描选项时，请注意标准 Web 筛选活动和实时扫描活动的记录方式有所不同。

针对标准 Web 筛选，您有若干选项可减少日志数据库的大小。

- 启用**访问次数**可为每个被请求的网站仅写入一个记录。请参阅*配置日志缓存文件*，第 263 页。
- 启用**合并**则可将多个含特定共同元素的请求合并入一个日志记录。请参阅*配置合并选项*，第 265 页。
- 禁用**完整 URL 记录**将仅记录每个请求的域名 (www.domain.com)，但不会记录至域内指定页面的路径 (/products/productA)。请参阅*配置完整 URL 记录*，第 273 页。
- 启用**选择类别记录**将仅记录对您的组织非常关键的选择类别。请参阅*配置 Filtering Service 以进行日志记录*，第 257 页。

但实时扫描功能仅在部分程度上受这些设置的限制。当实时扫描分析一个站点时，将会创建 2 个独立的日志记录。

- **网络筛选器记录**可利用任何已执行且可用于所有网络筛选器报告的大小缩减设置。
- **实时记录**将忽略大部分大小缩减设置。每次独立点击、对所有类别的请求都将被记录，且这些记录不会被合并处理。无论实时扫描后站点被阻止或允许，都将生成一份实时记录。对实时记录而言，仅完整 URL 记录的设置可被认为有效。

如果您已启用任何日志数据库大小缩减选项，则即使报告被配置为同样的用户、时间段和类别，实时报告中显示的数字可能也**无法**与标准筛选报告中的数字相匹配。例如，如果您已选择记录访问，且一名用户请求一个被实时扫描功能分析过的站点，则该用户的请求在标准筛选报告中将显示为一次访问，而在实时报告中将显示为多次点击。

要查看标准和实时筛选的比较数据，请**禁用**日志数据库大小缩减设置。因为此设置会导致数据库变得庞大并迅速膨胀，请确保日志数据库计算机拥有足够的硬盘、处理器和内存容量。

请参阅*报告管理*，第 253 页，以了解配置大小缩减设置的更多信息。请参阅*演示报告*，第 84 页和*调查报告*，第 100 页，以了解生成报告的有关信息。

8 Filter Remote 客户端

相关主题：

- *Remote Filtering 的运行方式*，第 134 页
- *配置 Remote Filtering 设置*，第 139 页

许多组织都有一些用户会将他们的便携式电脑带到网络外部使用。对于运行 Microsoft Windows 操作系统的远程用户，您可以通过执行 Websense Web Security 和 Websense Web Filter 的一项可选功能 Websense Remote Filtering 来筛选 Internet 请求。

Remote Filtering 监视 HTTP、 SSL 和 FTP 通信，它将应用分配到独立用户或组的策略，或者是默认策略，这具体取决于用户登录远程计算机的方式。 Remote Filtering 将不会根据分配到计算机或网络范围的策略进行筛选。请参阅 *识别远程用户*，第 137 页，以了解更多信息。

远程客户端不支持基于带宽的筛选 （请参阅 *使用 Bandwidth Optimizer 来管理带宽*，第 161 页）。带宽测量结果和报告中不包含远程流量生成的带宽。

FTP 和 SSL 请求的 Remote Filtering（例如 HTTPS）只能被阻止或允许。如果远程用户请求 FTP 站点或 HTTPS 站点，例如从已分配定额或确认操作的类别，则 Remote Filtering 客户端将被阻止访问该站点。当这些计算机从网络内部进行浏览时，会正常应用定额和确认筛选操作。

要执行 Remote Filtering，您必须安装下列组件：

- Remote Filtering Server 必须位于最外层的防火墙以内，且必须允许远程计算机与其进行通讯。通常情况下，它应安装在网络的*外围隔离区*或 DMZ，位于保护网络其余部分的防火墙外部。您最多可以安装 3 个 Remote Filtering Servers 来提供故障转移功能。

- Remote Filtering Client 必须位于运行 Windows 操作系统且在网络外部使用的计算机上。

> **注意**
> 请认真遵照*部署指南*中的建议来部署这些组件。请参阅*安装指南*以了解有关安装说明。
>
> 如果您是以独立模式（没有集成产品）使用 Websense，则应将 Network Agent 配置为不监视 Remote Filtering Server 计算机 （请参阅*配置全局设置*，第 290 页）。

Remote Filtering Client 和 Remote Filtering Server 之间的所有通讯均需经过身份验证且已加密。

Remote Filtering 的运行方式

相关主题：

- *网络内部*，第 135 页
- *网络外部*，第 136 页
- *识别远程用户*，第 137 页
- *在服务器通讯失败时*，第 137 页
- *虚拟专用网络 (VPN)*，第 138 页
- *配置 Remote Filtering 设置*，第 139 页

在远程计算机进行 HTTP、 SSL 或 FTP 请求时，其 Remote Filtering Client 会与 Remote Filtering Server 进行通讯。而 Remote Filtering Server 会与 Websense Filtering Service 进行通讯以确定要应用的操作。然后，Remote Filtering Server 将响应 Remote Filtering Client，要么允许该站点，要么发送相应的阻止消息。

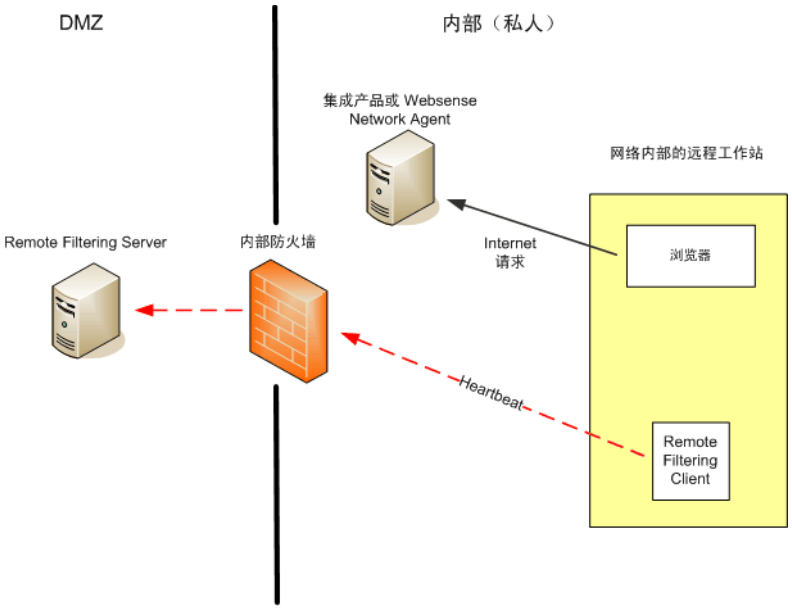
当运行 Remote Filtering Client 的计算机上的浏览器通过 HTTP、 SSL 或 FTP 进行请求时， Remote Filtering Client 必须决定是否要向 Remote Filtering Server 查询请求。这个决定是由计算机相对于网络的位置来控制的。

网络内部

相关主题：

- *Remote Filtering 的运行方式*，第 134 页
- *网络外部*，第 136 页
- *识别远程用户*，第 137 页
- *在服务器通讯失败时*，第 137 页
- *虚拟专用网络 (VPN)*，第 138 页
- *配置 Remote Filtering 设置*，第 139 页

当计算机在网络*内部*启动时， Remote Filtering Client 会尝试将**心跳信号 (heartbeat)** 发送到 DMZ 中的 Remote Filtering Server。由于 heartbeat 端口在内部防火墙上是打开的，因此 heartbeat 将会成功。



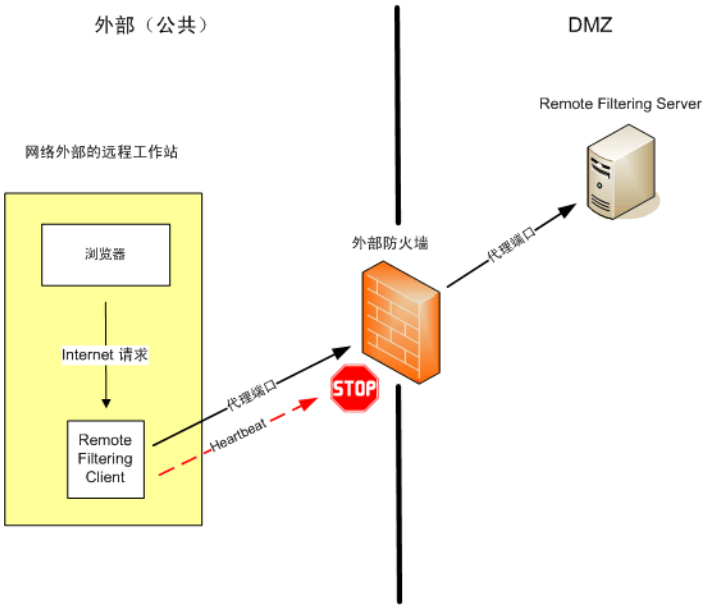
在这种情况下， Remote Filtering Client 将变为被动模式，不向 Remote Filtering Server 查询 Internet 请求。这些请求会被直接传送到集成产品（例如 Cisco Pix、Microsoft ISA Server）或 Websense Network Agent，然后像其他任何内部请求一样进行筛选。

网络外部

相关主题：

- *Remote Filtering 的运行方式*，第 134 页
- *网络内部*，第 135 页
- *识别远程用户*，第 137 页
- *在服务器通讯失败时*，第 137 页
- *虚拟专用网络 (VPN)*，第 138 页
- *配置 Remote Filtering 设置*，第 139 页

当计算机在网络*外部*启动时， Remote Filtering Client 会尝试向 Remote Filtering Server 发送 heartbeat。由于 heartbeat 端口在外部防火墙是被阻止的，因此 heartbeat 不会成功。



heartbeat 失败将提示 Remote Filtering Client 通过配置的端口 （默认为 80）将有关每个 HTTP、SSL 或 FTP 请求的查询发送到 DMZ 中的 Remote Filtering Server。然后， Remote Filtering Server 会将筛选请求转发到网络内部的 Websense Filtering Service。 Filtering Service 对请求进行评估，并将响应发送到 Remote Filtering Server。随后，响应将被发送至远程计算机。如果站点被阻止，则 Remote Filtering Client 会请求并接收相应的阻止页面，然后将阻止页面显示给用户。

Remote Filtering Client 会推迟每个筛选的请求，直到收到来自 Remote Filtering Server 的响应。根据收到的响应，Remote Filtering Client 要么允许站点，要么显示阻止页面。

日志文件可跟踪 Remote Filtering 活动，例如进入或离开网络、无法打开或关闭，以及重新启动客户端。 Remote Filtering Client 会在首次启动时创建日志文件。您可以控制是否显示此日志文件以及文件大小。请参阅*配置 Remote Filtering 设置*，第 139 页。

识别远程用户

相关主题：

- *Remote Filtering 的运行方式*，第 134 页
- *网络内部*，第 135 页
- *网络外部*，第 136 页
- *在服务器通讯失败时*，第 137 页
- *虚拟专用网络 (VPN)*，第 138 页
- *配置 Remote Filtering 设置*，第 139 页

用户登录远程计算机的方式将决定要实施的策略。

如果用户使用缓存的域凭据 （网络目录登录信息）登录，则 Websense Filtering Service 能够解析用户名，并将基于用户和组的相应策略应用到远程计算机。此外， Internet 活动将被记录在该网络用户名下。

如果用户使用计算机的本地用户帐户登录，则 Filtering Service 无法解析用户名，将应用默认策略。Internet 活动将被记录在本地用户名下。Remote Filtering 将不会根据分配到计算机或网络范围的策略进行筛选。

注意

如此处所述，对远程用户的筛选将始终根据远程用户的登录凭据进行。选择性身份验证设置不适用于这些用户。

在服务器通讯失败时

相关主题：

- *Remote Filtering 的运行方式*，第 134 页
- *网络内部*，第 135 页
- *网络外部*，第 136 页
- *识别远程用户*，第 137 页
- *虚拟专用网络 (VPN)*，第 138 页
- *配置 Remote Filtering 设置*，第 139 页

当网络外部的 Remote Filtering Client 成功地与网络 DMZ 中的 Remote Filtering Server 进行通讯时，将会进行筛选。但是，有时候可能会出现通讯不成功的情况。

当 Remote Filtering Client 无法联系 Remote Filtering Server 时将采取的操作是可配置的。默认情况下，Remote Filtering Client 会使用**无法打开**设置，该设置将在这些组件之间无法建立通讯时允许 HTTP、 SSL 和 FTP 请求。 Remote Filtering Client 会继续尝试联系 Remote Filtering Server。当通讯成功时，则会强制实施合适的筛选策略。

当 Remote Filtering Client 配置为**无法关闭**时，将应用超时值（默认为 15 分钟）。时钟在远程计算机启动时即开始运行。 Remote Filtering Client 会立即尝试连接 Remote Filtering Server，并不断循环尝试可用的 Remote Filtering Server 直到成功为止。

如果用户在启动时拥有 Web 访问，则在 Remote Filtering Client 连接 Remote Filtering Server 之前将不会进行筛选（所有请求都被允许）。连接后，将实施合适的筛选策略。

如果 Remote Filtering Client 在配置的超时时限内无法连接，则 Internet 访问将被阻止（失败则关闭），直到建立起与 Remote Filtering Server 之间的连接。

注意

如果 Remote Filtering Server 出于某些原因无法连接到 Websense Filtering Service，则会向 Remote Filtering Client 返回一个错误，筛选将始终无法打开。

此超时时限允许在旅行中为 Internet 访问付费的用户启动计算机并安排连接，而不会被锁定。如果用户在 15 分钟的超时时限过期之前没有建立 Web 访问，则在该会话期间无法建立 Web 访问。出现这种情况时，用户必须重新启动计算机以再次开始超时间隔。

要更改无法打开/失败则关闭设置和超时值，请参阅*配置 Remote Filtering 设置*，第 139 页。

虚拟专用网络 (VPN)

相关主题：

- *Remote Filtering 的运行方式*，第 134 页
- *网络内部*，第 135 页
- *网络外部*，第 136 页
- *识别远程用户*，第 137 页
- *在服务器通讯失败时*，第 137 页
- *配置 Remote Filtering 设置*，第 139 页

Websense Remote Filtering 支持 VPN 连接，包括 隧道分离 VPN。当远程计算机通过 VPN （非隧道分离）连接到内部网络时， Remote Filtering Client 可以向 Remote Filtering Server 发送 heartbeat。然后，Remote Filtering Client 将变为被动模式，来自远程计算机的所有 HTTP、 SSL 和 FTP 请求都会由内部集成产品或 Network Agent 进行筛选，就像其他网络内计算机一样。

如果远程计算机通过隧道分离的 VPN 连接到内部网络，则 Remote Filtering Client 会检测到这一点，因此不会向 Remote Filtering Server 发送 heartbeat。 Remote Filtering Client 将假定它在外部运行并将请求提交至 Remote Filtering Server 进行筛选。

Websense 软件支持下列 VPN 客户端的隧道分离：

- Checkpoint SecureClient
- Cisco
- Juniper/Netscreen
- Microsoft PPTP
- Nokia
- Nortel
- SonicWALL

配置 Remote Filtering 设置

相关主题：

- *Remote Filtering 的运行方式*，第 134 页
- *网络内部*，第 135 页
- *网络外部*，第 136 页
- *识别远程用户*，第 137 页
- *在服务器通讯失败时*，第 137 页
- *虚拟专用网络 (VPN)*，第 138 页

无限制超级管理员可以使用**设置 > 常规 > Remote Filtering** 页面来配置选项，这些选项会影响与此安装有关的所有 Remote Filtering Clients。

有关 Remote Filtering 运行方式的详细信息，请参阅 *Remote Filtering 的运行方式*，第 134 页。

1. 选中**失败则关闭**复选框可阻止 Remote Filtering Clients 进行所有 Internet 访问，除非其计算机正在与 Remote Filtering Server 进行通讯。

   默认情况下，该复选框未被选中，这就意味着远程用户在其计算机无法与 Remote Filtering Server 通讯时可以对 Internet 进行未筛选的访问。

2. 如果您勾选 “失败则关闭”选项，请使用**失败则关闭超时**字段来选择最多为 60 的分钟数 （默认为 15）或选择**无超时**。

   在超时时限内，所有 HTTP、 SSL 和 FTP 请求都是允许的。

   在超时间隔内，如果 Remote Filtering Client 无法与 Remote Filtering Server 进行通讯，则所有 Internet 访问都将被阻止 （失败则关闭）。

选择**无超时**可以在用户能够从酒店或其他使用付费提供商建立 Internet 连接之前锁定远程计算机。此外， Remote Filtering Client 会不断尝试与 Remote Filtering Server 进行通讯。

警告

Websense, Inc. 不推荐选择**无超时**或将超时时限设置为极低的数字。

3. 选择**本地日志缓存的最大大小**（MB），最多为 10。选择**无日志**将禁用日志记录。

   这可以在远程计算机最初与 Remote Filtering Server 断开连接时控制日志文件的大小和是否启用日志文件。此日志文件将跟踪以下事件：

   - 计算机离开网络
   - 计算机重新加入网络
   - Remote Filtering Client 启动
   - 出现无法打开的情况
   - 出现失败则关闭的情况
   - Remote Filtering Client 接收策略更新

   计算机将保留 2 个最新的日志。这些日志可用于对 Remote Filtering 的连接问题或其他问题进行故障诊断。

9 改善筛选策略

按最简单的方式配置时， Internet 使用筛选只需配置一项单一策略，一周 7 天，一天 24 小时应用一个类别筛选器和一个协议筛选器。而 Websense 软件则为您提供远比此基本筛选功能强大的工具，从而能更精确地达到您对 Internet 使用的管理粒度要求。您可以：

- 创建**受限访问筛选器**以阻止某些用户对特定列表以外站点的访问 （请参阅*限制用户只能访问已定义列表中的 Internet 站点*，第 141 页）。
- 创建**自定义类别**以重新定义对选择的站点的筛选方式（请参阅*使用类别*，第 147 页）。
- **重新分类 URL** 可将特定的站点从其默认的类别移动至其他由 Websense 定义的类别或自定义类别中 （请参阅*重新分类 URL*，第 155 页）。
- 定义**未筛选的 URL** 以允许用户可访问特定网站，无论其是否已被分配至活动类别筛选器中阻止的类别中 （请参阅*定义未筛选的 URL*，第 154 页）。
- 在带宽使用情况达到特定阈值之时，实施**带宽**限制以阻止用户访问未达阈值时允许的类别和协议。
- 在关键字阻止启用和激活时，定义**关键字**以用于阻止在关键字阻止未启用和激活时允许的类别中的站点 （请参阅*根据关键字筛选*，第 151 页）。
- 在文件类型阻止被激活时，定义**文件类型**以用于阻止文件类型阻止未激活时允许的类别中的选定文件类型的下载（请参阅*根据文件类型管理通信*，第 163 页）。

限制用户只能访问已定义列表中的 Internet 站点

相关主题：

- *受限访问筛选器和筛选优先权*，第 142 页
- *创建受限访问筛选器*，第 143 页
- *编辑受限访问筛选器*，第 144 页

受限访问筛选器是一种非常精确的 Internet 访问筛选方法。每一个受限访问筛选器都是一个独立网站的列表。和类别筛选器一样，受限访问筛选器需添加至策略才能在指定时间段内实施。策略内的受限访问筛选器被激活后，被分配至该策略的用户将只能对列表中的站点进行访问，而所有其他站点都将被阻止。

例如，假设 First Grade 策略实施了只包含特定教育和参考站点的受限访问筛选器，则受该 First Grade 策略控制的学生将只能访问这些站点，而不能访问任何其他站点。

重要

当使用某个受限访问筛选器时，Websense 软件将只对请求的站点是否存在于筛选器中进行检查，而不会对任何其他项目进行检查。

这意味着即使某个筛选器允许的站点已被恶意代码感染，无论该站点的 Master Database 或实时扫描类别如何，用户对该站点的访问请求都将被允许。

激活受限访问筛选器后，对未包括在该筛选器内的任何 URL 的请求都将返回一个阻止页面。

Websense 软件最多可支持 2,500 个受限访问筛选器，总计可包含 25,000 个 URL。

受限访问筛选器和筛选优先权

在某些情况下，单一用户可适用多个筛选策略。例如，当用户同时属于多个受不同策略制约的组时，就会发生上述情况。此外，出现在受限访问筛选器中的 URL 也可同时被定义为未筛选的 URL。

当用户适用多个组的策略时，**使用更强限制性的阻止**设置（请参阅*筛选顺序*，第 68 页）将决定该用户被筛选的方式。默认情况下，该设置为关闭。

Websense 软件将从筛选器层面来确定哪种筛选设置的限制性较弱。如果用户受多种策略制约且其中之一正实施受限访问筛选器，则“限制性较弱”的类别有时可能会有所不同。

当**使用更强限制性的阻止**为**关闭**时：

- 如**全部阻止**类别筛选器和受限访问筛选器同时适用，则受限访问筛选器通常被认定为限制性较弱。
- 如同时适用的是任何其他的类别筛选器和受限访问筛选，则类别筛选器将被认定为限制性较弱。

  也就是说，当受限访问筛选器允许而类别筛选器阻止某个站点时，该站点将被阻止。

当**使用更强限制性的阻止**为**打开**时，则受限访问筛选器将被认定为除“全部阻止”以外的限制性最强的筛选器。

下方表格对多项策略同时适用时，**使用更强限制性的阻止**设置对筛选产生的影响进行了汇总：

	使用更强限制性的阻止 **关闭**	*使用更强限制性的阻止* **打开**
受限访问筛选器 + **全部阻止**类别筛选器	受限访问筛选器（允许的请求）	**全部阻止**（阻止的请求）
受限访问筛选器 + 允许的类别	类别筛选器（允许的请求）	受限访问筛选器（允许的请求）
受限访问筛选器 + 阻止的类别	类别筛选器（阻止的请求）	受限访问筛选器（允许的请求）
受限访问筛选器 + 定额/确认类别	类别筛选器（按定额限制的请求/确认）	受限访问筛选器（允许的请求）
受限访问筛选器 + 未筛选的 URL	未筛选的 URL（允许的请求）	受限访问筛选器（允许的请求）

创建受限访问筛选器

相关主题：

- *筛选器使用*，第 42 页
- *限制用户只能访问已定义列表中的 Internet 站点*，第 141 页
- *编辑受限访问筛选器*，第 144 页

使用**添加受限访问筛选器**页面（可通过**筛选器**或**编辑策略**页面来访问）可为您的新筛选器指定唯一名称和描述。创建筛选器后，请输入允许的 URL 列表并将筛选器分配至某项策略，然后对客户端应用该策略。

1. 输入一个唯一的**筛选器名称**。名称长度必须介于 1 至 50 个字符之间，且不得包含下列符号：

   ```
   * < > { } ~ ! $ % & @ # . " | \ & + = ? / ; : ,
   ```

   筛选器名称中可以包含空格、连接线和省略符号。
2. 输入筛选器的简短**描述**。此描述会出现在筛选器页面受限访问筛选器的筛选器名称旁边，应能够解释筛选器的目的，从而帮助管理员随时间变化管理策略。

   筛选器名称的字符限制也适用于描述之中，但有 2 项例外：描述可包括句点 (.) 和逗号 (,)。
3. 要查看和编辑新的筛选器，请单击**确定**。要放弃更改并返回筛选器页面，请单击**取消**。

新的受限访问筛选器创建完成后，将被添加至**策略管理 > 筛选器 > 受限访问筛选器**列表中。单击某个筛选器名称可编辑该筛选器。

要完成对新筛选器的自定义，请继续*编辑受限访问筛选器*。

编辑受限访问筛选器

相关主题：

- *限制用户只能访问已定义列表中的 Internet 站点*，第 141 页
- *受限访问筛选器和筛选优先权*，第 142 页
- *创建受限访问筛选器*，第 143 页
- *编辑策略*，第 66 页

受限访问筛选器是由网站（URL 或 IP 地址）和正则表达式组成的列表，可用于指定用户可访问的特定站点。当筛选器被应用至客户端时，这些客户端将无法访问不在列表之中的任何站点。

重要

当使用某个受限访问筛选器时， Websense 软件将只对请求的站点是否存在于筛选器中进行检查，而不会对任何其他项目进行检查。

这意味着即使某个筛选器允许的站点已被恶意代码感染，无论该站点的 Master Database 或实时扫描类别如何，用户对该站点的访问请求都将被允许。

使用**策略管理 > 筛选器 > 编辑受限访问筛选器**页面可对现有的受限访问筛选器进行更改。您可更改筛选器的名称和描述、查看已执行该筛选器的策略列表以及对筛选器中所包含的站点进行管理。

当您编辑受限访问筛选器时，所作的更改会影响执行该筛选器的每一项策略。

1. 因此请仔细确认筛选器的名称和描述。要更改筛选器名称，请单击**重命名**，然后输入新名称。则新名称将被更新至所有已执行该受限访问筛选器的策略中。
2. 利用**使用此筛选器的策略**字段可查看当前正在执行此筛选器的策略数量。如有 1 个或多个策略执行该筛选器，则单击**查看策略**可将这些策略列出。
3. 在“添加或删除站点”中输入要添加至受限访问筛选器中的 URL 和 IP 地址。每一行输入一个 URL 或 IP 地址。

   HTTP:// 前缀可不必输入。

   当根据站点的 Master Database 类别对其进行筛选时， Websense 软件将把 URL 以及与其相等价的 IP 地址进行匹配。但使用受限访问筛选器时情况不同。要允许某个站点的 URL 和 IP 地址，需将两者都添加至筛选器中。
4. 单击右侧的箭头 (>) 可将 URL 和 IP 地址移动至允许的站点列表中。
5. 除了可将单个站点添加至受限访问筛选器外，您还可添加与多个站点匹配的正则表达式。要创建正则表达时，请单击**高级**。
   - 每行输入一个正则表达式，然后单击右侧的箭头将表达式移动至允许的站点列表中。

- 要验证某个正则表达式是否与预期站点相匹配，请单击**测试**。
- 请参阅*使用正则表达式*，第 165 页，以获得使用正则表达式进行筛选的详细信息。

6. 查看**允许的站点**列表中的 URL、 IP 地址和正则表达式。
   - 要对某个站点或正则表达式进行更改，请将其选中并单击**编辑**。
   - 要从列表中删除某个站点或正则表达式，请将其选中并单击**删除**。
7. 在编辑筛选器之后，请单击**确定**，将您的更改存入缓存中并返回筛选器页面。直到您单击**全部保存**之后，更改才会生效实施。

从编辑策略页面添加站点

相关主题：

- *限制用户只能访问已定义列表中的 Internet 站点*，第 141 页
- *受限访问筛选器和筛选优先权*，第 142 页
- *创建受限访问筛选器*，第 143 页
- *编辑策略*，第 66 页

使用**策略 > 编辑策略 > 添加站点**页面可将站点添加至受限访问筛选器中。

每一行输入一个 URL 或 IP 地址。如果您没有指定协议，则 Websense 软件将会自动添加 **HTTP://** 前缀。

完成更改之后，请单击**确定**返回 “编辑策略” 页面。您还须单击 “编辑策略” 页面上的**确定**以缓存更改。直到您单击**全部保存**之后，更改才会生效实施。

对受限访问筛选器所做的更改将影响所有执行该筛选器的策略。

将筛选器和策略复制到角色

相关主题：

- *创建类别筛选器*，第 43 页
- *创建协议筛选器*，第 45 页
- *创建受限访问筛选器*，第 143 页
- *创建策略*，第 65 页

超级管理员可使用**筛选器 > 复制筛选器到角色**和**策略 > 复制策略到角色**页面将一个或多个筛选器或角色复制到所委派的管理员角色。一旦筛选器或策略被复制后，委派管理员即可使用这些筛选器或策略来对他们所管理的客户端进行筛选。

- 在目标角色中，选项卡 （“已复制”）将添加到筛选器或策略名称的结尾。如果同一筛选器或策略被复制了多次，则名称中还将添加复制的次数。
- 委派管理员可对已复制到其角色的筛选器或策略进行重命名或编辑。
- 已复制到某个委派管理员角色的类别筛选器将把该角色创建的自定义类别的筛选操作设置为 “允许” 。因此，委派管理员应更新被复制的类别筛选器，从而为其角色特定的自定义类别设置所需操作。
- 委派管理员对由超级管理员复制到其角色的筛选器或策略进行的更改不会对超级管理员的原始筛选器或策略或任何其他接收该筛选器或策略副本的角色产生影响。
- 筛选器锁定限制也不会对超级管理员的原始筛选器或策略产生影响，但会对委派管理员的筛选器或策略副本产生影响。
- 由于委派管理员受到 “筛选器锁定” 限制的影响，因此 “全部允许” 类别和协议筛选器无法被复制到委派管理员角色。

要复制筛选器或策略：

1. 请在 “复制筛选器到角色” 或 “复制策略到角色” 页面中确认显示在页面顶部列表中的策略或筛选器是否正确。
2. 使用**选择角色**下拉列表来选择一个目标角色。
3. 单击**确定**。

   弹出式对话框会指明所选的筛选器或策略已被复制。复制过程可能会需要一段时间。

   直到您单击**全部保存**之后，更改才会生效实施。

复制过程完成后，选定角色的委派管理员可在再次登录 Websense Manager 后访问所复制的筛选器或策略。如果复制筛选器或策略时，委派管理员已登录至拥有策略访问权限的角色，则他们在注销并再次登录之前将无法查看这些新的筛选器或策略。

构建筛选器组件

使用**策略管理 > 筛选器组件**页面可访问用于改善和自定义 Websense 软件执行贵组织 Internet 访问策略方式的工具。屏幕上的 4 个按钮分别对应以下任务：

编辑类别	• 重新分类 URL （请参阅*针对特定站点重新定义筛选*，第 153 页）。例如，如果 “购物”类别被您的 Internet 筛选策略所阻止，而您又想允许对特定供应商或合作伙伴站点的访问，则可将这些站点添加至某个允许的类别，如 “商业与经济”类别）。 • 定义或编辑自定义类别（请参阅*创建自定义类别*，第 150 页）。在 Websense 定义或用户定义的父类别中创建其他的子类别，然后将 URL 分配至这些新类别中。 • 将关键字分配到类别 （请参阅*根据关键字筛选*，第 151 页） 。要对 URL 中包含特定字符串的站点进行重新分类并阻止对它们的访问，首先请定义相应的关键字，然后在某个类别筛选器中启用关键字阻止。 • 创建可用于匹配多个 URL 的正则表达式（请参阅*使用正则表达式*，第 165 页）、模式或模板，然后将它们分配到某个类别。
编辑协议	定义或编辑自定义协议定义（请参阅*创建自定义协议*，第 159 页和*编辑自定义协议*，第 157 页）。例如，如果贵组织的成员使用了某种自定义的消息工具，则您可通过创建一个自定义的协议定义以允许使用该工具的同时阻止其他即时消息发送协议。
文件类型	创建或编辑文件类型定义以用于阻止允许的类别中的特定文件类型 （请参阅*根据文件类型管理通信*，第 163 页）。
未筛选的 URL	定义允许所有客户端访问的特定站点，无论其是否属于阻止的类别 （请参阅*定义未筛选的 URL*，第 154 页）。请注意，将 URL 添加至此列表不会覆盖 “全部阻止”类别筛选器或受限访问筛选器。

使用类别

相关主题：

- *编辑类别及其属性*，第 148 页
- *创建自定义类别*，第 150 页
- *根据关键字筛选*，第 151 页
- *针对特定站点重新定义筛选*，第 153 页

Websense 软件为筛选不在 Master Database 内的站点和更改 Master Database 内的单个站点的筛选的方式提供了多种方法。

- 创建**自定义类别**可进行更为精确的筛选和报告操作。
- 使用**重新分类的 URL** 可为未分类的站点定义类别，或更改 Master Database 中显示的站点的类别。
- 定义**关键字**可将所有 URL 中包含特定字符串的站点进行重新分类。

编辑类别及其属性

相关主题：

- *创建自定义类别*，第 150 页
- *查看所有自定义类别属性*，第 149 页
- *更改全局类别筛选*，第 149 页
- *根据关键字筛选*，第 151 页
- *针对特定站点重新定义筛选*，第 153 页

使用**策略管理 > 筛选器组件 > 编辑类别**页面可创建并修改自定义类别、重新分类的 URL 和关键字。

现有类别（包括 Websense 定义和自定义类别）均会在内容窗格的左侧部分中列出。要查看与类别相关的当前自定义设置，或创建新的自定义定义，请首先从列表中选择一个类别。

要查看全部自定义 URL、关键字，以及与全部类别相关的正则表达式的列表，请单击页面顶部工具栏中的**查看所有自定义 URL /关键字**。请参阅*查看所有自定义类别属性*，第 149 页，以了解更多信息。

- 要创建新类别，请单击**添加**，然后转至*创建自定义类别*，第 150 页，以获得进一步的说明。

  要删除现有的自定义类别，请选择类别，然后单击**删除**。您不能删除 Websense 定义的类别。
- 要更改自定义类别的名称或描述，请选中该类别然后单击**重命名**（请参阅*重命名自定义类别*，第 150 页）。
- 要在全部类别筛选器中更改与一个类别相关的筛选操作，请单击**覆盖操作**（请参阅*更改全局类别筛选*，第 149 页）。
- **重新分类的 URL** 列表将显示已被分配到此类别的重新分类的站点（URL 和 IP 地址）。
  - 要将某个站点添加至列表，请单击**添加 URL**。请参阅*重新分类 URL*，第 155 页，以获得进一步的说明。
  - 要更改现有的重新分类站点，请选择 URL 或 IP 地址，然后单击**编辑**。
- **关键字**列表将显示与此类别相关联的关键字。

- 要定义与选择的类别相关联的关键字，请单击**添加关键字**。请参阅*根据关键字筛选*，第 151 页，以获得进一步的说明。
- 要更改现有的关键字定义，请选择关键字，然后单击**编辑**。

◆ 除了 URL 和关键字以外，您还可为类别定义**正则表达式**。每个正则表达式都是一个可用于将多个站点与类别相关联的模式或模板。

要查看或为类别创建正则表达式，请单击**高级**。

- 要定义正则表达表达式，请单击“添加表达式”（请参阅*使用正则表达式*，第 165 页）。
- 要更改现有的正则表达式，请选择表达式，然后单击**编辑**。

◆ 要删除重新分类的 URL、关键字或正则表示式，请选择要删除的项，然后单击**删除**。

完成对“编辑类别”页面的更改后，请单击**确定**以缓存更改并返回“筛选器组件”页面。直到您单击**全部保存**之后，更改才会生效实施。

查看所有自定义类别属性

使用**筛选器组件 > 编辑类别 > 查看所有自定义 URL 和关键字**页面可查看 URL、关键字和正则表达式的定义。您还可删除不再需要的定义。

该页面包含 3 个相类似的表格，每种类别属性一个：自定义 URL、关键字或正则表达式。在各个表格中，属性将被列在与之相关联的类别名称的旁边。

要删除类别属性，请选择相应的复选框，然后单击**删除**。

要返回“编辑类别”页面，请单击**关闭**。如果您已删除“查看所有自定义和关键字”页面上的项，请单击“编辑类别”页面上的**确定**以缓存更改。直到您单击**全部保存**之后，更改才会生效实施。

更改全局类别筛选

使用**筛选器组件 > 编辑类别 > 覆盖操作**页面可在所有现有类别筛选器中更改应用于类别的操作。此外，还可确定新筛选器中的类别将应用的默认操作。

虽然此更改可覆盖所有现有筛选器中的某个类别所应用的操作，但管理员还在日后编辑这些筛选器以应用不同的操作。

更改类别应用的筛选设置之前，请先确认**选择的类别**旁显示的类别名称是否正确。然后，您可以：

1. 选择一个新的**操作**（允许、阻止、确认或定额）。请参阅*筛选操作*，第 39 页，以了解更多信息。

   默认情况下，页面上所有选项都选择了**不要更改当前设置**。
2. 指定是否要**阻止关键字**。请参阅*根据关键字筛选*，第 151 页，以了解更多信息。
3. 指定是否要**阻止文件类型**，并自定义阻止设置。请参阅*根据文件类型管理通信*，第 163 页，以了解更多信息。

4. 在**高级筛选**中，指定是否要使用 Bandwidth Optimizer 来管理对 HTTP 站点的访问并自定义阻止设置。请参阅*使用 Bandwidth Optimizer 来管理带宽*，第 161 页，以了解更多信息。

   重要
   在此页面进行的更改将对**全部阻止**和**全部允许**之外的现有类别筛选器产生影响。

5. 单击**确定**返回“编辑类别”页面（请参阅*编辑类别及其属性*，第 148 页）。直到您单击“编辑类别”页面上的**确定**之后，更改才会缓存。

重命名自定义类别

使用**筛选器组件 > 编辑类别 > 重命名类别**页面可更改与某个自定义类别相关联的名称和描述。

- 使用**筛选器名称**字段可编辑类别名称。新名称必须唯一，且不得超过 50 个字符。

  名称中不得包含以下字符：

  ```
  * < > { } ~ ! $ % & @ # . " | \ & + = ? / ; : ,
  ```

- 使用**描述**字段可编辑类别描述。描述不得超过 255 个字符。

  筛选器名称的字符限制也适用于描述之中，但有 2 项例外：描述可包括句点 (.) 和逗号 (,)。

完成更改之后，请单击**确定**返回“编辑类别”页面。直到您单击“编辑类别”页面上的**确定**之后，更改才会缓存。

创建自定义类别

相关主题：

- *编辑类别及其属性*，第 148 页
- *根据关键字筛选*，第 151 页
- *针对特定站点重新定义筛选*，第 153 页

除使用 Master Database 中 90 多种 Websense 定义的类别之外，您还可定义自己的**自定义类别**，从而进行更为精确的筛选和报告操作。例如，创建如下自定义类别：

- **商务旅行**，以对合格供应商的站点进行分组，从而令员工可通过这些站点购买机票、租赁车辆和预定酒店
- **参考资料**，以对在线词典和百科全书站点进行分组，从而令其中的站点适合小学学生使用。
- **职业发展**，以对鼓励员工访问以提高其技能的培训站点和其他资源进行分组。

使用**策略管理 > 筛选器组件 > 编辑类别 > 添加类别**页面可将自定义类别添加到任何父类别。您最多可创建 100 个自定义类别。

1. 输入一个唯一的描述性**筛选器名称**，名称中不得包含以下字符：

   ```
   * < > { } ~ ! $ % & @ # . " | \ & + = ? / ; : ,
   ```

2. 输入新类别的**描述**。

   筛选器名称的字符限制也适用于描述之中，但有 2 项例外：描述可包括句点 (.) 和逗号 (,)。

3. 从**添加到**列表中选择父类别。默认情况下，**所有类别**将被选中。
4. 输入要添加到此类别的站点 （URL 或 IP 地址）。请参阅*重新分类 URL*，第 155 页，以了解更多信息。

   您也可在创建类别后编辑此列表。
5. 输入您想与此类别相关联的关键字。请参阅*根据关键字筛选*，第 151 页，以了解更多信息。

   您也可在创建类别后编辑此列表。
6. 定义默认筛选**操作**从而在所有现有的类别筛选器中将其应用到此类别。日后，您可在单个筛选器中编辑此操作。

   注意

   已复制到某个委派管理员角色的类别筛选器将把该角色创建的自定义类别的筛选操作设置为 “允许” 。因此，委派管理员应更新被复制的类别筛选器，从而为其角色特定的自定义类别设置所需操作。

7. 在所有现有的类别筛选器中启用需被应用于此类别的所有**高级筛选**操作（关键字阻止、文件类型阻止或带宽阻止）。
8. 定义新类别完成后，请单击**确定**以缓存更改并返回至“编辑类别”页面。直到您单击**全部保存**之后，更改才会生效实施。

新类别将被添加至 “类别”列表，并将显示该类别的自定义 URL 及关键字的信息。

根据关键字筛选

相关主题：

- *重新分类 URL*，第 155 页
- *配置 Websense 筛选设置*，第 49 页
- *创建类别筛选器*，第 43 页
- *编辑类别筛选器*，第 43 页
- *使用类别*，第 147 页

关键字与类别相关联，并用于提供针对未明确纳入 Master Database 或定义为自定义 URL 的站点的保护。必须执行三个步骤以启用关键字筛选：

1. 全局启用关键字筛选 （请参阅*配置 Websense 筛选设置*，第 49 页）。
2. 定义与类别相关联的关键字 （请参阅*定义关键字*，第 152 页）。
3. 在活动的类别筛选器中针对该类别启用关键字阻止 （请参阅*编辑类别筛选器*，第 43 页）。

当正对特定类别定义关键字并启用关键字筛选时，Websense 软件将对所有 URL 中包含某个关键字的站点加以阻止，并将这些站点记录为属于这一指定类别。即使属于同一类别的其他 URL 是允许的，这些站点也会被阻止。

例如，如果在某个活动的类别筛选器中，“体育”类别是允许的，而您又想阻止对篮球站点的访问，则可将关键字 “nba”与 “体育”相关联，并启用关键字阻止。这意味着以下 URL 将被阻止，并被记录为属于 “体育”类别：

- sports.espn.go.com/**nba**/
- moder**nba**kery.com
- moder**nba**biesandchildren.com
- fashio**nba**r.com

请谨慎定义关键字，以免出现不必要的过度阻止。

重要

如果您正在使用 Websense Web Security，则应避免将关键字与任何 “扩展保护”子类别相关联。这些类别无法执行关键字阻止。

在某个请求因关键字而被阻止时，相关信息将显示在用户接收到的 Websense 阻止页面上。

定义关键字

相关主题：

- *编辑类别筛选器*，第 43 页
- *使用类别*，第 147 页
- *根据关键字筛选*，第 151 页
- *使用正则表达式*，第 165 页

关键字是一个可在 URL 中找到的字符串 （如单词、短语或缩写）。将关键字分配到某个类别，然后在类别筛选器中启用关键字阻止。

使用**策略管理 > 筛选器组件 > 编辑类别 > 添加关键字**页面可将关键字与类别相关联。如果您需要更改关键字定义，请使用**编辑关键字**页面。

定义关键字时，应谨慎定义以免出现不必要的过度阻止。例如，您可能想通过关键字“sex”来阻止对成人网站的访问，但结果却是阻止了搜索引擎对“sextuplets”或“City of Essex”等词的请求，以及对诸如 m**sex**change.org（信息技术）、vega**sex**perience.com（旅行）和 sci.esa.int/mar**sex**press（教育机构）等站点的请求。

每行输入一个关键字。

- 关键字内不得包含空格。 URL 和 CGI 字符串单词之间不包括空格。
- 请在诸如以下特殊字符之前添加一个反斜线 (\):

  . , # ? * +

  如果您未添加反斜线，则 Websense 软件将忽略这些特殊字符。
- 如果您正在使用 Websense Web Security，则应避免将关键字与任何“扩展保护”子类别相关联。这些类别无法执行关键字阻止。

添加或编辑关键字完成后，请单击**确定**以缓存更改并返回至“编辑类别”页面。直到您单击**全部保存**之后，更改才会生效实施。

为执行关键字阻止，您还必须：

1. 通过**设置 > 筛选**页面来启用关键字阻止（请参阅*配置 Websense 筛选设置*，第 49 页）。
2. 为一个或多个活动的类别筛选器中启用关键字阻止（请参阅*编辑类别筛选器*，第 43 页）。

针对特定站点重新定义筛选

相关主题：

- *创建自定义类别*，第 150 页
- *根据关键字筛选*，第 151 页
- *定义未筛选的 URL*，第 154 页
- *重新分类 URL*，第 155 页

利用自定义 URL，您可以：

- 对不包括在 Websense Master Database 之内的站点应用更为精确的筛选。默认情况下，应用于 **Miscellaneous\Uncategorized** 类别的操作将被用于对这些站点进行筛选。
- 采用与 Master Database 类别不同的方式筛选站点

在查询 Master Database 之前，Websense 软件会先查找站点的自定义 URL 定义，并根据分配到自定义 URL 的类别对站点进行筛选。

自定义 URL 的类型有两种：未筛选的重新分类 URL。

- 所有不受 “全部阻止” 类别筛选器或受限访问筛选器控制的用户都可访问 “未筛选的 URL”（请参阅*定义未筛选的 URL*，第 154 页）。
- 而重新分类 URL 已从其 Master Database 类别移动至其他 Websense 定义的类别或自定义类别中 （请参阅*重新分类 URL*，第 155 页）。

  默认情况下重新分类 URL 将不会被阻止，而其筛选将根据在每个活动的类别筛选器中的新类别所应用的操作来进行。

当根据站点的 Master Database 类别对其进行筛选时， Websense 软件将把 URL 以及与其相等价的 IP 地址进行匹配。但针对自定义 URL 时情况不同。要更改站点被筛选的方式，需将其 URL 和 IP 地址同时定义为自定义 URL。

如果站点能通过多个 URL 来访问，则请将所有能用于访问该站点的 URL 都定义为自定义 URL，以确保站点能按预期被允许或阻止。

如果站点被移往新的域，并使用 HTTP 重定向来将用户转至新的 URL，则由于新的 URL 不会自动按照与重定向站点相同的方式进行筛选，因此要确保该站点的新地址也能得到相应的筛选，请创建一个新的自定义 URL。

定义未筛选的 URL

相关主题：

- *使用类别*，第 147 页
- *针对特定站点重新定义筛选*，第 153 页
- *重新分类 URL*，第 155 页

使用**策略管理 > 筛选器组件 > 未筛选的 URL** 页面可在受到 “全部阻止” 类别筛选器或受限访问筛选器控制之外的情况下，定义可被任何用户访问的站点的列表。

内容窗格右侧的**允许的站点**列表中将列出您已定义的未筛选的站点（URL 和 IP 地址）和正则表达式 （请参阅*使用正则表达式*，第 165 页）。每个站点都将与一个类别相关联。

- 而 URL 则既可与其 Master Database 类别相关联，也可以是重新分类的。
- 若用户请求访问未筛选的 URL，则请求将在该 URL 被分配的类别中被记录为允许的自定义 URL。

要添加未筛选的 URL：

1. 在**定义未筛选的 URL** 中，每一行输入一个 URL 或 IP 地址，然后单击右侧的箭头 (>)。

   Websense 软件不会将自定义 URL 及与其等价 IP 地址进行匹配。要同时允许某个站点的 URL 和 IP 地址，请将它们都添加到 “未筛选的 URL” 列表中。

2. 要添加与多个站点相匹配的正则表达式，请单击**高级**。每行输入一个正则表达式，然后单击右侧的箭头将表达式移动至 “未筛选的 URL” 列表中。要验证某个模式是否与预期站点相匹配，请单击**测试**。

   请参阅 *使用正则表达式*，第 165 页，以了解详细信息。

3. 在完成之后，单击**确定**以缓存您的更改并返回 “编辑类别” 页面。直到您单击**全部保存**之后，更改才会生效实施。

要从 “未筛选的 URL” 列表中删除站点，请选择该站点的 URL、 IP 地址或正则表达式，然后单击**删除**。

重新分类 URL

相关主题：

- *使用类别*，第 147 页
- *针对特定站点重新定义筛选*，第 153 页
- *定义未筛选的 URL*，第 154 页

使用**策略管理 > 筛选器组件 > 编辑类别 > 重新分类 URL** 页面可向任何类别添加单个站点。对**编辑重新分类 URL** 页面上的现有重新分类站点进行更改。

重新分类 URL 可更改某个站点被筛选和记录的方式。当您添加重新分类的站点时：

- 每行输入一个 URL 或 IP 地址。
- 为非 HTTP 站点输入协议。若协议空缺，则 Websense 软件将把该站点视为 HTTP 站点来进行筛选。

  针对 HTTPS 站点，还应输入端口号 （https://63.212.171.196:443/、 https://www.onlinebanking.com:443/）。
- Websense 软件将严格根据自定义 URL 输入的信息来对其进行识别。如果 “搜索引擎与门户” 类别被阻止，而您又将 **www.yahoo.com** 重新分类为允许的类别，则只有当用户键入完整地址时，该站点才可被访问。如果用户键入 images.search.yahoo.com 或 yahoo.com，则该站点仍将被阻止。如果您将 **yahoo.com** 重新分类，则所有地址中包含 yahoo.com 的站点都将被允许。

添加或编辑重新分类站点完成后，请单击**确定**以缓存更改并返回至 “编辑类别” 页面。直到您单击**全部保存**之后，更改才会生效实施。

保存完重新分类 URL 后，请使用右侧快捷窗格中的 **URL 类别**工具以验证站点是否已被分配至正确的类别。请参阅 *工具箱可用于验证筛选行为*，第 166 页。

使用协议

Websense Master database 包含的协议定义可用于对 HTTP、 HTTPS 和 FTP 以外的其他 Internet 协议进行筛选。这些定义包括各种 Internet 应用程序和数据传输方法，例如用于即时通信、流媒体、文件共享、文件传送、 Internet 邮件及其他网络和数据库操作的应用程序和传输方法。

这些协议定义甚至可用于对能以隧道方式通过 HTTP 通信常用端口绕过防火墙的协议或应用程序进行筛选。例如，即时消息数据就能以隧道方式通过 HTTP 端口来进入防火墙设置为阻止即时消息协议的网络。 Websense 软件可准确地识别这些协议，并根据您配置的策略对它们进行筛选。

注意

Network Agent 是启用基于协议的筛选所必需的。

除使用 Websense 定义的协议定义外，您还可定义自定义协议以用于筛选。自定义协议定义可根据 IP 地址或端口号进行，并可进行编辑。

要阻止特定端口的通信，请将该端口号与某个自定义协议相关联，然后为该协议分配默认的**阻止**操作。

要使用自定义协议定义，请转至**策略管理 > 筛选器组件**，然后单击**协议**。有关详细信息，请参阅*编辑自定义协议*，第 157 页和*创建自定义协议*，第 159 页。

筛选协议

相关主题：

- *使用协议*，第 156 页
- *编辑自定义协议*，第 157 页
- *创建自定义协议*，第 159 页
- *添加或编辑协议标识符*，第 158 页
- *添加至 Websense 定义的协议*，第 161 页

在已安装 Network Agent 的情况下，Websense 软件可对通过特定端口传输的、或使用特定 IP 地址或标记有特定标志的 Internet 内容进行阻止，而与数据的性质如何无关。默认情况下，不论其来源如何，对某个端口的阻止将拦截所有通过该端口进入您的网络的 Internet 内容。

注意

有时，即使使用特定端口的协议已被阻止，通过该端口发送的内部网络通信可能不会被阻止，因为协议通过内部服务器发送数据的速度比 Network Agent 捕获与处理数据的速度要快。但针对源自网络外部的数据这种情况不会发生。

请求协议时， Websense 软件将根据以下步骤来决定对请求的阻止或允许：

1. 确定协议 （或 Internet 应用程序）名称。
2. 识别基于请求目标地址的协议。
3. 在自定义协议定义中搜索相关的端口号和 IP 地址。
4. 在 Websense 定义的协议定义中搜索相关的端口号、 IP 地址或标志。

如果 Websense 软件无法确定上述信息，则所有与该协议相关的内容都将被允许。

编辑自定义协议

相关主题：

- *使用协议*，第 156 页
- *创建自定义协议*，第 159 页
- *创建协议筛选器*
- *编辑协议筛选器*
- *使用类别*

使用**策略管理 > 筛选器组件 > 编辑协议**页面可创建和编辑自定义协议定义，并查看 Websense 定义的协议定义，但无法编辑 Websense 定义的协议。

“协议”列表将包括所有自定义和 Websense 定义的协议。单击协议或协议组，可在内容窗格的右侧部分获得选择的项目的相关信息。

要添加新的自定义协议，请单击**添加协议**，然后继续*创建自定义协议*，第 159 页。

要编辑协议定义：

1. 在 “协议”列表中选择某个协议。则该协议定义将显示在列表右侧。
2. 单击**覆盖操作**可更改所有协议筛选器中应用于该协议的筛选操作 （请参阅*更改全局协议筛选*，第 159 页）。
3. 单击**添加标识符**可为此协议定义其他协议标识符 （请参阅*添加或编辑协议标识符*，第 158 页）。
4. 在列表中选择一个标识符，然后单击**编辑**可对由该标识符定义的**端口** 、**IP 地址范围**或**传输方法**进行更改。
5. 在完成后，请单击**确定**以缓存您的更改。直到您单击**全部保存**之后，更改才会生效实施。

要删除协议定义，请在协议列表中选择要删除的项，然后单击**删除**。

添加或编辑协议标识符

使用**筛选器组件 > 编辑协议 > 添加协议标识符**页面可为现有的自定义协议定义其他的协议标识符。使用**编辑协议标识符**页面可对之前定义的标识符进行更改。

在创建或更改标识符之前，请确认**选择的协议**旁显示的协议名称是否正确。

使用协议标识符时，请谨记每个协议都必须有至少一项唯一的标准 （端口、 IP 地址或传输类型）。

1. 指定该标识符要包括的**端口**。
   - 如果您选择**所有端口**，则该标准将与其他协议定义中输入的其他端口或 IP 地址发生重叠。
   - 一旦出现重叠，则端口范围就不被视为唯一。例如，端口范围 80-6000 就与范围 4000-9000 发生重叠，
   - 则在定义端口为 80 或 8080 的协议时就应谨慎进行。由于 Network Agent 将通过这些端口来侦听 Internet 请求，

     而且自定义协议优先于 Websense 协议，因此如果您使用端口 80 来定义自定义协议，则所有也使用端口 80 的其他协议也都将按自定义协议的方式来进行筛选和记录。
2. 指定该标识符要包括的 **IP 地址**。
   - 如果您选择**所有外部 IP 地址**，则该标准将与其他协议定义中输入的任何其他 IP 地址发生重叠。
   - 一旦出现重叠，则 IP 地址范围就不被视为唯一。
3. 指定此标识符要包括的**协议传输**方式。
4. 单击**确定**以缓存您的更改，然后返回 “编辑协议”页面。直到您单击**全部保存**之后，更改才会生效实施。

重命名自定义协议

使用**筛选器组件 > 编辑协议 > 重命名协议**页面可更改自定义协议的名称，或将之移动至不同的协议组。

- 使用**名称**字段可编辑协议名称。新名称不得超过 50 个字符。

  名称中不得包含以下字符：

  ```
  * < > { } ~ ! $ % & @ # . " | \ & + = ? / ; : ,
  ```
- 要将协议移动至其他协议组，请从**在组中**字段中选择一个新的组。

完成更改之后，请单击**确定**返回 “编辑协议”页面。您还须单击 “编辑协议”页面上的**确定**以缓存更改。

更改全局协议筛选

使用**筛选器组件 > 编辑协议 > 覆盖操作**页面可对所有现有的协议筛选器中协议被筛选的方式进行更改。此外，还可确定新筛选器中的协议将应用的默认操作。

虽然此更改可覆盖应用于所有现有的协议筛选器的筛选操作，但管理员还在日后编辑这些筛选器以应用不同的操作。

1. 确认**选择的协议**旁显示的协议名称是否正确。
2. 选择要应用于此协议的新**操作**（允许或阻止）。默认情况下，**不更改**将被选中。请参阅*筛选操作*，第 39 页，以了解更多信息。
3. 指定新的**记录**选项。协议通信必须被记录及显示于报告中，并启用协议使用警报。
4. 明确是否已使用 **Bandwidth Optimizer** 来管理对此协议的访问。请参阅*使用 Bandwidth Optimizer 来管理带宽*，第 161 页，以了解更多信息。

   重要
   在此页面进行的更改将对**全部阻止**和**全部允许**之外的现有协议筛选器产生影响。

5. 完成之后，请单击**确定**返回“编辑协议”页面（请参阅*编辑自定义协议*，第 157 页）。您还须单击“编辑协议”页面上的**确定**以缓存更改。

创建自定义协议

相关主题：

- *使用协议*，第 156 页
- *筛选协议*，第 156 页
- *编辑自定义协议*，第 157 页
- *添加至 Websense 定义的协议*，第 161 页

使用**筛选器组件 > 协议 > 添加协议**页面可定义新的自定义协议。

1. 输入协议**名称**。

   名称中不得包含以下字符：

   ```
   * < > { } ~ ! $ % & @ # . " | \ & + = ? / ; : ,
   ```

   可为自定义协议分配与 Websense 定义协议相同的名称，以扩展与原始协议相关联的 IP 地址或端口的数量。请参阅*添加至 Websense 定义的协议*，第 161 页，以了解更多信息。
2. 展开**向该组添加协议**下拉列表，然后选中某个协议组。则在所有协议列表和筛选器中，新的协议将显示在该组之中。

3. 为该组定义一个唯一的**协议标识符**（**端口**、**IP 地址**和**传输方法**的集合）。您可在日后从 “编辑协议” 页面添加其他的标识符。

   请在创建协议标识符时认真遵照以下这些指南：

   - 每个协议定义必须有至少一个标准 （端口、 IP 地址或传输类型）是唯一的。
   - 如果您选择**所有端口**或**所有外部 IP 地址**，则该标准将与其他协议定义中输入的任何其他端口或 IP 地址发生重叠。
   - 一旦出现重叠，则端口或 IP 地址范围就不被视为唯一。例如，端口范围 80-6000 就与范围 4000-9000 发生重叠，

   注意

   则在定义端口为 80 或 8080 的协议时就应谨慎进行。由于 Network Agent 将通过这些端口来侦听 Internet 请求。

   而且自定义协议优先于 Websense 协议，因此如果您使用端口 80 来定义自定义协议，则所有也使用端口 80 的其他协议也都将按自定义协议的方式来进行筛选和记录。

   以下表格将为您提供一些有效和无效协议定义的示例：

端口	IP 地址	传输方法	可接受的组合？
70	任意	TCP	是的，所使用的端口号令各协议标识符都是唯一的。
90	任意	TCP	

端口	IP 地址	传输方法	可接受的组合？
70	任意	TCP	不， IP 地址不唯一。“任意” 集合中包含 10.2.1.201。
70	10.2.1.201	TCP	

端口	IP 地址	传输方法	可接受的组合？
70	10.2.3.212	TCP	是的，IP 地址是唯一的。
70	10.2.1.201	TCP	

4. 在 “默认筛选操作” 中，指定应在所有活动的协议筛选器中应用于此协议的默认操作 （**允许**或**阻止**）：
   - 指明使用此协议的通信是否应加以**记录**。协议通信必须被记录及显示于报告中，并启用协议使用警报。
   - 指明对此协议的访问是否应受 **Bandwidth Optimizer** 的控制（请参阅 *使用 Bandwidth Optimizer 来管理带宽*，第 161 页）。

5. 完成之后，请单击**确定**返回“编辑协议”页面。新的协议定义将出现在“协议”列表中。
6. 再次单击**确定**以缓存您的更改。直到您单击**全部保存**之后，更改才会生效实施。

添加至 Websense 定义的协议

您无法直接向 Websense 定义的协议添加端口号或 IP 地址。但您可以创建与 Websense 定义的协议名称相同的自定义协议，然后向其定义中添加端口或 IP 地址。

当自定义协议与 Websense 定义的协议具有相同名称时，Websense 软件将在两个定义指定的端口和 IP 地址中查找协议通信。

报告中，自定义协议的名称带有 “C_” 前缀。例如，如果您为 SQL_NET 创建了一个自定义协议并指定了其他的端口号，则当协议使用自定义协议中的端口号时报告将显示 C_SQL_NET。

使用 Bandwidth Optimizer 来管理带宽

相关主题：

- *使用类别*，第 147 页
- *使用协议*，第 156 页
- *配置默认的 Bandwidth Optimizer 限制*，第 162 页

创建类别或协议筛选器时，您可选择根据带宽使用情况来限制对类别或协议的访问。

- 根据网络带宽的总体使用阻止对类别或协议的访问。
- 根据 HTTP 通信的总体带宽使用阻止对类别的访问。
- 根据特定协议所使用的带宽阻止对该协议的访问。

例如：

- 当网络带宽的总体使用超过可用带宽的 50% 或当前 AIM 带宽使用超过网络总带宽的 10% 时， AOL 即时消息协议将被阻止。
- 当总体带宽使用已达到 75% 或所有 HTTP 通信的带宽使用达到可用网络带宽的 60% 时，“体育”类别将被阻止。

协议带宽使用包括流经针对该协议定义的所有端口、 IP 地址或标志的通信。这意味着当协议或 Internet 应用程序使用多个端口进行数据传输时，流经协议定义所包括的端口的通信都将被计入该协议的总体带宽使用。但如果 Internet 应用程序使用的端口不包括在协议定义中，则通过该端口的通信将不会被包括在带宽使用中。

Websense 软件将记录经筛选的基于 TCP 和 UDP 的协议所使用的带宽。

Websense, Inc. 将定期更新 Websense 协议定义以确保带宽计算的准确性。

Network Agent 将按预定的间隔向 Filtering Service 发送网络带宽数据。这将确保 Websense 软件可精确监视带宽使用，并获得最接近平均数值的测量数据。

当基于带宽的筛选选项被激活时， Websense 软件将在初始化配置完成后 10 分钟以及各 Websense Policy Server 重新启动后 10 分钟时开始基于带宽的筛选。这一延时将确保准确地衡量带宽数据和在筛选中使用该数据。

当请求因带宽限制而被阻止时， Websense 阻止页面的**原因**字段中将显示这一信息。更多信息，请参阅*阻止页面*，第 73 页。

配置默认的 Bandwidth Optimizer 限制

相关主题：

- *编辑类别筛选器*，第 43 页
- *编辑协议筛选器*，第 46 页
- *使用 Bandwidth Optimizer 来管理带宽*，第 161 页

在指定策略中的带宽设置之前，请确认触发基于带宽的筛选设置的默认带宽阈值。 Websense 定义的值为：

- 默认网络带宽：**50%**
- 每个协议的默认带宽：**20%**

默认带宽值将由 Policy Server 进行存储，并由所有 Network Agent 的相关实例来加以执行。如果您有多台 Policy Server，则对一台 Policy Server 上的默认带宽值的更改不会影响其他 Policy Server。

要更改默认带宽值：

1. 在 Websense Manager 中，转至**设置 > 筛选**。
2. 输入将触发基于带宽的筛选 （前提是带宽筛选已启用）的带宽使用阈值。
   - 若针对整个网络根据通信阻止类别或协议，则默认筛选阈值将由**默认网络带宽**来决定。
   - 若针对某个协议根据通信阻止类别或协议，则默认筛选阈值将由**每个协议的默认带宽**来决定。

   您可在任何类别或协议筛选器中覆盖每个类别或协议的默认阈值。
3. 在完成后，请单击**确定**以缓存您的更改。直到您单击**全部保存**之后，更改才会生效实施。

对默认设置所作的更改可能会对其他执行 Bandwidth Optimizer 限制的类别和协议筛选器产生影响。

- 要管理与特定协议相关联的带宽使用，请编辑活动的协议筛选器或筛选器。
- 要管理与特定 URL 类别相关联的带宽使用，请编辑相应的类别筛选器或筛选器。

  当您根据 HTTP 带宽使用筛选类别时， Websense 软件将针对所有 HTTP 端口使用的总体 HTTP 带宽进行计算。

根据文件类型管理通信

创建类别筛选器时，您可以根据文件扩展名定义的筛选，并限制对特定类别站点中特定文件类型的访问。例如，允许“体育”类别，但是阻止站点上的“体育”类别的视频文件。

Websense 软件为您提供多种预定义文件类型及用途类似的文件扩展名组。这些文件类型定义都保存在 Master Database 中，并可作为 Master Database 更新过程的一部分而进行更改。

您可利用预定义的文件类型执行筛选、修改现有的文件类型定义或创建新的文件类型。但请注意，您无法删除 Websense 定义的文件类型或与之相关的文件扩展名。

当用户申请站点时， Websense 软件会首先确定该站点的类别，然后对要筛选的文件扩展名进行检查。

注意

要对视频和音频的 Internet 媒体执行完全筛选，需将基于协议和基于文件类型的筛选结合起来进行。这种情况下，协议筛选将负责流媒体的筛选，而文件类型筛选则负责可下载并播放的文件的筛选。

当用户尝试访问扩展名被阻止的文件时， Websense 阻止页面上的**原因**字段将指明该文件类型是被阻止的。更多信息，请参阅*阻止页面*，第 73 页。

注意

如果阻止的 GIF 或 JPEG 图片仅是某个允许的页面的一部分，则不会显示标准的阻止页面，而是将图片区域显示为空白。这将避免在允许的页面上的多个位置同时显示阻止页面的其中一小部分。

文件类型定义所包括的文件扩展名将视筛选目的所需而定，数量可能有多有少。例如， Websense 定义文件类型将包含以下文件扩展名：

音频	压缩的文件		可执行文件	视频	
.aif	.ace	.mim	.bat	.asf	.mpg
.aifc	.arc	.rar	.exe	.asx	.mpv2
.aiff	.arj	.tar		.avi	.qt
.m3u	.b64	.taz		.ivf	.ra

音频	压缩的文件		可执行文件	视频	
.mid	.bhx	.tgz		.m1v	.ram
.midi	.cab	.tz		.mov	.wm
.mp3	.gz	.uu		.mp2	.wmp
.ogg	.gzip	.uue		.mp2v	.wmv
.rmi	.hqx	.xxe		.mpa	.wmx
.snd	.iso	.z		.mpe	.wxv
.wav	.jar	.zip			
.wax	.lzh				
.wma					

任何与 Websense 定义的文件类型相关联的文件扩展名均可被添加至自定义的文件类型中。然后这些文件扩展名将根据与自定义文件类型相关联的设置来进行筛选和记录。

要查看现有的文件类型定义、编辑文件类型或创建自定义文件类型，请转至**策略管理 > 筛选器组件**，然后单击**文件类型**。请参阅*使用文件类型*，第 164 页，以了解更多信息。

使用文件类型

相关主题：

- *根据文件类型管理通信*，第 163 页
- *编辑类别筛选器*，第 43 页
- *筛选站点*，第 69 页

使用**策略管理 > 筛选器组件 > 编辑文件类型**页面可创建和管理多达 32 种的**文件类型**。文件类型指在类别筛选器中可被明确阻止的文件扩展名的组（请参阅*根据文件类型管理通信*，第 163 页）。

- 单击一个文件类型可查看与类型相关的文件扩展名。
- 要向选择的文件类型中添加扩展名，请单击**添加扩展名**，然后请参阅*向文件类型中添加文件扩展名*，第 165 页，以获得进一步的说明。
- 要创建新的文件类型，请单击**添加文件类型**，然后请参阅*添加自定义文件类型*，第 165 页，以获得进一步的说明。
- 要删除自定义的文件类型或扩展名，请选择相应的项，然后单击**删除**。

  您无法删除 Websense 定义的文件类型或与之相关的文件扩展名。

  但您可将与 Websense 定义的文件类型相关的文件扩展名添加至自定义的文件类型中。然后这些文件扩展名将根据与自定义文件类型相关联的设置来进行筛选和记录。您无法向多个自定义文件类型中添加同一个扩展名。

完成文件类型定义的修改后，请单击**确定**。直到您单击**全部保存**之后，更改才会生效实施。

添加自定义文件类型

使用**筛选器组件 > 编辑文件类型 > 添加文件类型**页面可定义自定义文件类型。

1. 输入一个唯一的**文件类型名称**，

   您可创建与 Websense 定义的文件类型名称相同的自定义文件类型，从而向现有的文件类型中添加其他的文件扩展名。
2. 在**用户定义的文件扩展名**列表中每行输入一个文件扩展名。每个扩展名前可不必输入圆点 （“.”）。
3. 单击**确定**返回“编辑文件类型”页面。新的文件类型将显示在“文件类型”列表中。
4. 文件类型定义完成后，请单击“编辑文件类型”页面上的**确定**。直到您单击**全部保存**之后，更改才会生效实施。

向文件类型中添加文件扩展名

使用**筛选器组件 > 编辑文件类型 > 添加文件扩展名**页面可向选择的文件类型中添加文件扩展名。

1. 确认**选择的文件类型**旁显示的文件类型名称是否为预期名称。
2. 在**文件扩展名**列表中每行输入一个文件扩展名。每个扩展名前可不必输入圆点 （“.”）。
3. 单击**确定**返回 “编辑文件类型”页面。新的文件扩展名将显示在自定义文件扩展名列表中。
4. 文件类型定义完成后，请单击“编辑文件类型”页面上的**确定**。直到您单击**全部保存**之后，更改才会生效实施。

使用正则表达式

正则表达式就是用于匹配多个字符串或字符组的模板或模式。您可在受限访问筛选器使用正则表达式，或用其定义自定义 URL 或关键字。然后 Websense 筛选将尝试为其匹配通用的模式，而不是特定的单个 URL 或关键字。

请考虑下面这个简单的正则表达式：

```
domain.(com|org|net)
```

该表达式模式将匹配以下 URL：

- domain.com
- domain.org
- domain.net

应谨慎使用正则表达式，因为它们虽然可提供强有力的筛选工具，但也很容易导致某些站点不按预期设置被阻止或允许。此外，若正则表达式未被恰当构建，还可能会导致筛选过度。

重要

将正则表达式作为筛选标准可能会增加 CPU 使用率。测试显示在使用 100 个正则表达式的情况下，Filtering Service 计算机的平均 CPU 使用率会提高 20%。

Websense 软件支持大多数的正则表达式 Perl 语法，但也有一些例外。部分语法不被支持是因为它们无法有效匹配 URL 中可能出现的字符串。

不支持的正则表达式语法包括：

```
(?<=pattern)string
(?<!pattern)string
\N{name}
(?imsx-imsx)
(?(condition)pat1)
\pP
(?(condition)pat1|pat2)
\PP
(?{code})
??{code})
```

有关正则表达式的更多帮助，请参阅：

en.wikipedia.org/wiki/Regular_expression

www.regular-expressions.info/

工具箱可用于验证筛选行为

Websense Manager 的右侧快捷窗格中包含一个可用于快速验证筛选设置的**工具箱**。

单击工具名称即可访问该工具。再次单击名称则可显示工具的列表。有关工具使用的更多信息，请参阅：

- *URL 类别*，第 167 页
- *查看策略*，第 167 页
- *测试筛选*，第 167 页
- *URL 访问*，第 168 页
- *调查用户*，第 168 页

您还可单击**支持门户**以在新的浏览器选项卡或窗口中访问 Websense 技术支持网站。您可利用支持门户中的知识库来访问相关的教程、提示、文章和文档。

URL 类别

要查看站点当前的分类方式：

1. 单击工具箱中的 **URL 类别**。
2. 输入一个 URL 或 IP 地址。
3. 单击**开始**。

则该站点的当前类别将显示在弹出式窗口中。如果您的组织已对 URL 进行重新分类，则会显示它的新类别。

站点的类别可能会根据您所使用的 Master Database （包括实时更新）版本不同而有所不同。

查看策略

使用此工具可确定特定客户端所应用的策略。所显示的结果是当前日期和时间下的策略应用情况。

1. 单击工具箱中的 **查看策略**。
2. 要识别目录或计算机客户端，请输入：
   - 完全符合条件的用户名

     要浏览或搜索目录以识别用户，请单击**查找用户**（请参阅 *识别用户以查看策略或测试筛选*，第 168 页）。
   - IP 地址
3. 单击**开始**。

则一个或多个策略的名称将显示在弹出式窗口中。只有当用户未被分配任何策略，而用户所属的多个组、域或组织单位被分配策略时，才会显示多个策略。

但是，即使显示多个策略，在任何给定时间内一名用户也只可适用一种策略（请参阅 *筛选顺序*，第 68 页）。

测试筛选

要查看特定客户端请求特定站点时所会发生什么情况：

1. 单击工具箱中的 **测试筛选**。
2. 要识别目录或计算机客户端，请输入：
   - 完全符合条件的用户名

     要浏览或搜索目录以识别用户，请单击**查找用户**（请参阅 *识别用户以查看策略或测试筛选*，第 168 页）。
   - IP 地址
3. 输入要测试的站点的 URL 或 IP 地址。
4. 单击**开始**。

则站点类别、应用至类别的操作以及操作原因将显示在弹出式窗口中。

URL 访问

要查看用户在过去 2 周 （包括今天）内是否曾尝试访问站点：

1. 单击工具箱中的 **URL 访问**。
2. 输入要测试的站点的全部或部分 URL 或 IP 地址。
3. 单击**开始**。

此时会显示一份调查报告，表明站点是否曾被访问，如果是，则会显示时间。

您可以在接到安全警报后使用这项工具，查看您的组织是否已经接触了网络钓鱼或感染病毒的网站。

调查用户

要查看客户端在过去 2 周 （不包括今天）内的 Internet 使用历史记录：

1. 单击工具箱中的**调查用户**。
2. 输入全部或部分用户名或计算机 IP 地址。
3. 单击**开始**。

此时会显示一份包含客户历史记录的调查报告。

识别用户以查看策略或测试筛选

使用**查找用户**页面可为 “查看策略” 或 “测试筛选” 工具识别用户 （目录）客户端。

该页面将在选择**用户**选项后打开。展开 **Directory Entries** 文件夹以浏览目录，或单击**搜索**。只有当您使用基于 LDAP 的目录服务时，才可使用搜索功能。

要搜索目录以查找用户：

1. 输入全部或部分的用户**名称**。
2. 展开 **Directory Entries** 树以浏览并指定一个搜索上下文。

   您必须单击树中的文件夹（DC、OU 或 CN）才可指定上下文，该操作将填写树下方的字段。
3. 单击**搜索**。与搜索条件相匹配的项将列在**搜索结果**下方。
4. 单击用户名可选择其中一个用户，或单击**重新搜索**以输入新的搜索条件或上下文。

   要返回并浏览目录，请单击**取消搜索**。
5. 当完全合格的用户名正确显示在**用户**字段中时，单击**开始**。

如果您正使用 “测试筛选” 工具，请在单击**开始**前确保 **URL** 字段中所显示的 URL 或 IP 地址正确无误。

要识别计算机客户端而不是用户客户端，请单击 **IP 地址**。

10 用户标识

要将策略应用至用户和组，Websense 软件必须能通过给定的源 IP 地址，来识别正在进行请求的用户。可供使用的识别方式有多种：

- 由已集成的设备或应用程序来识别和验证用户的身份，然后再将用户信息传递给 Websense 软件。更多信息，请参阅*安装指南*。
- 由工作于后台并对 Websense 透明的标识代理来与目录通讯和识别用户（请参阅*透明标识*）。
- 由 Websense 软件来提示用户输入他们的网络凭据并在他们打开网络浏览器时要求他们进行登录 （请参阅*手动身份验证*，第 170 页）。

透明标识

相关主题：

- *手动身份验证*，第 170 页
- *配置用户标识方式*，第 171 页

一般而言，**透明标识**指的是可供 Websense 软件用于识别目录服务中用户的那些所有无需提示用户输入登录信息的方式。具体包括：已与 Websense 软件集成并可提供可供筛选使用的用户信息之设备或应用程序，或者可选的 Websense 透明标识代理。

- Websense *DC Agent*, 第 178 页可与基于 Windows 的目录服务配合使用。其代理将定期向域控制器查询用户的登录会话，然后对客户端计算机进行轮询以确认登录的状态。它可运行在 Windows 服务器上，并可安装在网络上的任一域中。
- Websense *Logon Agent*, 第 181 页将在用户登录 Windows 域时对其进行识别。其代理既可运行在 Linux 上也可运行在 Windows 服务器上，但只能与运行在 Windows 计算机上的登录应用程序相关联。
- Websense *RADIUS Agent*, 第 183 页可与基于 Windows 或 LDAP 的目录服务配合使用。其代理将与 RADIUS 服务器和客户端相配合，以识别来自远程位置的用户登录。

- Websense *eDirectory Agent*, 第 187 页可与 Novell eDirectory 配合使用。其代理将使用 Novell eDirectory 的身份验证来建立用户与 IP 地址之间的映射。

关于各类代理的安装说明，请参阅*安装指南*。代理既可单独使用，也可按一定组合来使用 （请参阅*配置多个代理*，第 192 页）。

> **注意**
>
> 如有使用集成的 NetCache 设备，则 NetCache 必须以 WinNT、 LDAP 或 RADIUS 格式向 Websense 软件发送用户名称，才能令透明识别正常工作。
>
> 如设置有代理服务器且使用了透明标识代理，则最好将代理服务器的身份验证设置为匿名。

一般用户标识设置和特定透明标识代理都可通过 Websense Manager 管理器来进行配置。单击位于左侧导航窗格中的**设置**选项卡，然后单击**用户标识**。

详细的配置说明，请参阅*配置用户标识方式*, 第 171 页。

在某些情况下， Websense 软件可能会无法自透明标识代理处获得用户信息。例如：当有多个用户被分配至同一计算机、用户是匿名用户或访客，以及出现一些其他的原因时。在这些情况下，您可以提示用户应通过浏览器来登录 （请参阅*手动身份验证*，第 170 页）。

远程用户的透明标识

通过一定的配置， Websense 软件也可透明地识别自远程位置登录网络的用户。

- Websense 软件可通过部署 Websense Remote Filtering Server 和 Remote Filtering Client 来识别使用域账户登录某个已缓存的域的所有远程用户。更多信息，请参阅 *Filter Remote 客户端*，第 133 页。
- 如已部署 DC Agent，则 DC Agent 将可以识别那些直接登录网络中的已命名 Windows 域的用户 （请参阅 *DC Agent*，第 178 页）。
- 如使用 RADIUS 服务器对来自远程位置的用户登录进行身份验证，则 RADIUS Agent 可透明识别这些用户，从而令您能根据用户或组来应用筛选策略（请参阅 *RADIUS Agent*，第 183 页）。

手动身份验证

相关主题：

- *透明标识*，第 169 页
- *为特定的计算机设置身份验证规则*，第 173 页
- *安全手动身份验证*，第 175 页
- *配置用户标识方式*，第 171 页

不是所有环境都可以或适宜使用透明标识。对尚未使用透明标识的组织或无法使用透明标识的情况下，您仍然可以通过**手动身份验证**来按照基于用户和组的策略进行过滤。

手动身份验证将在用户首次通过浏览器来访问 Internet 时提示其输入用户名和密码。Websense 软件将通过所支持的目录服务来确认其密码，然后检索该用户适用的策略信息。

您既可在透明标识不可用时随时将 Websense 软件配置为启用手动身份验证（请参阅*配置用户标识方式*，第 171 页），也可创建一个使用自定义身份验证设置的计算机的列表，当用户在这些计算机上打开浏览器时将被提示登录（请参阅*为特定的计算机设置身份验证规则*，第 173 页）。

启用手动身份验证后，如出现以下情况之一，则用户将遇到 HTTP 错误并将无法访问 Internet：

- 用户尝试输入密码失败 3 次，即用户名或密码无效。
- 用户单击**取消**以绕过身份验证提示。

启用手动身份验证后，无法识别的用户将不能浏览 Internet。

配置用户标识方式

相关主题：

- *透明标识*，第 169 页
- *手动身份验证*，第 170 页
- *使用用户和组*，第 54 页

请使用**设置 > 用户标识**页面来管理软件应于何时及如何来尝试识别网络中的用户，以应用基于用户和组的策略。

- 配置 Policy Server 与透明标识代理进行通讯。
- 检查并更新透明标识代理的设置。
- 设置全局规则来决定，当透明标识代理或已集成的设备无法识别用户时，Websense 软件应作何回应。
- 识别网络中的哪些计算机不适用全局用户标识规则，并指定这些计算机的用户是否要以及应如何进行身份验证。

如果您使用的是透明标识代理，则这些代理将列于**透明标识代理**之下：

- **服务器**显示驻留透明标识代理的计算机的 IP 地址或名称。
- **端口**显示 Websense 软件用来与代理通讯的端口。
- **类型**标明指定实例的类型是否为：DC Agent、Logon Agent、RADIUS Agent 或 eDirectory Agent（对各代理类型的介绍，请参阅*透明标识*, 第 169 页）。

要向该列表中添加代理，请先从**添加代理**下拉列表中选择代理类型。单击以下链接之一以了解配置说明：

- *配置 DC Agent*，第 179 页
- *配置 Logon Agent*，第 181 页
- *配置 RADIUS 代理*，第 185 页
- *配置 eDirectory Agent*，第 189 页

要自列表中删除代理，先在列表中勾选代理信息一侧的复选框，然后单击**删除**。

在**其他身份验证选项**下，指定当用户未（由代理或集成）进行透明识别时，Websense 软件应作出的默认回应：

- 单击**应用计算机或网络策略**来忽略基于用户和组的策略，并应用基于计算机或网络的策略，或默认策略。
- 单击**提示用户输入登录信息**来要求用户在打开浏览器时提供登录凭据。然后即可应用基于用户和组的策略（请参阅*手动身份验证*，第 170 页）。
- 指定在用户被提示输入登录凭据时，Websense 软件应使用的默认域**上下文**，即用户凭据有效的域。

  如已使用例外列表来指定其上用户将被提示输入登录信息的计算机，则必须提供一个默认的域上下文，即便全局规则的设置将应用基于计算机或网络的策略。

在创建将决定 Websense 软件应于何时和以何种方式来识别用户的一般规则后，您还可以为该规则创建一些例外。

例如，假设您使用透明标识代理或集成产品来识别用户，并已激活手动身份验证从而能在无法对用户进行透明标识时提示他们输入凭据，然后您还可以指定一些特定的计算机，在这些计算机上：

- 无法被识别的用户将不会被提示输入其凭据。换句话说，当透明标识失败后，将不会进行手动身份验证，并将应用基于计算机或网络的策略，或默认策略。
- 即使可用，用户信息也将总是被忽略，且用户将一直被提示输入其凭据。
- 即使可用，用户信息也将总是被忽略，且用户将不会被提示输入其凭据（并将始终应用基于计算机或网络的策略，或默认策略）。

要创建例外，请单击**例外**，然后请参阅*为特定的计算机设置身份验证规则*，第 173 页。

在完成对此页面的更改后，请单击**确定**以保存更改。如要取消保存更改，则请单击**取消**。

为特定的计算机设置身份验证规则

相关主题：

- *配置用户标识方式*，第 171 页
- *手动身份验证*，第 170 页
- *安全手动身份验证*，第 175 页

选择性身份验证将使您可以决定从某一特定客户端计算机（通过 IP 地址来识别）请求 Internet 访问的用户是否将收到通过浏览器输入用户登录凭据的提示。这可被用于：

- 为公共信息亭中的计算机，而不是提供该信息亭之组织的员工建立不同的身份验证规则
- 确保诊所检查室中计算机的用户在获得 Internet 访问之前必须通过识别。

采用特定用户标识设置的计算机将被列在**设置 > 用户标识**页面中。单击**例外**可为网络中的某些计算机创建特定的用户标识设置，或查看特定计算机是否已定义特别设置。

要向列表中添加计算机，请单击**添加**，然后请参阅 *定义用户标识设置的例外*，第 173 页以获得进一步的说明。

在完成向列表添加计算机或网络范围之后，请单击**确定**。直到您单击**全部保存**之后，更改才会生效实施。

定义用户标识设置的例外

相关主题：

- *透明标识*，第 169 页
- *手动身份验证*，第 170 页
- *配置用户标识方式*，第 171 页

通过**设置 > 用户标识 > 添加 IP 地址**页面可确定哪些计算机需应用特定的用户标识规则。

1. 输入一个 **IP** 地址或 **IP 地址范围**可确定哪些计算机需应用特定的身份验证方式，然后单击向右的箭头将它们添加至**已选择**列表中。

   如同一规则需应用至多台计算机，则请将它们全部添加入列表。
2. 在**用户标识**下拉列表中选择一项来标明 Websense 软件是否应尝试透明识别这些计算机的用户。
   - 选择**尝试透明识别用户**可从透明标识代理或集成设备请求用户信息。
   - 选择**忽略用户信息**可避免使用任何透明方式来识别用户。

3. 标明是否要提示用户通过浏览器来输入登录凭据。此设置将于用户信息不可用、其他识别方式失败或忽略用户信息时应用。
   - 选择**提示用户输入登录信息**可要求用户提供登录凭据。

     如**尝试透明识别用户**也被选中，则用户将只会在无法进行透明标识时收到浏览器提示。
   - 选择**应用计算机或网络策略**可确保用户绝对不会被要求提供登录凭据。

     如**尝试透明识别用户**也被选中，则所持凭据无法通过透明标识的用户将会被相应的基于用户的策略过滤掉。
4. 单击**确定**以返回用户标识页面。
5. 在更新例外列表之后，请单击**确定**来缓存您的更改。直到您单击**全部保存**之后，更改才会生效实施。

修订用户标识设置的例外

相关主题：

- *透明标识*，第 169 页
- *手动身份验证*，第 170 页
- *配置用户标识方式*，第 171 页

使用**设置 > 用户标识 > 编辑 IP 地址**页面可对例外列表中的项进行更改。对此页面的更改将对“已选择”列表中的所有计算机（按 IP 地址或范围来识别）产生影响。

1. 在**用户标识**下拉列表中选择一项来标明 Websense 软件是否应尝试透明识别这些计算机的用户。
   - 选择**尝试识别用户**可从透明标识代理或集成设备请求用户信息。
   - 选择**忽略用户信息**可避免使用任何透明方式来识别用户。
2. 标明是否要提示用户通过浏览器来输入登录凭据。此设置将于用户信息不可用、透明标识失败或忽略透明标识时应用。
   - 选择**提示用户输入登录信息**可要求用户提供登录凭据。

     如**尝试识别用户**也被选中，则用户将只会在无法进行透明标识时收到浏览器提示。
   - 选择**应用计算机或网络策略**可确保用户绝对不会被要求提供登录凭据。

     如**尝试识别用户**也被选中，则所持凭据无法通过透明标识的用户将会被相应的基于用户的策略过滤掉。
3. 单击**确定**以返回用户标识页面。
4. 在更新例外列表之后，请单击**确定**来缓存您的更改。直到您单击**全部保存**之后，更改才会生效实施。

安全手动身份验证

相关主题：

- *配置用户标识方式*，第 171 页
- *手动身份验证*，第 170 页
- *为特定的计算机设置身份验证规则*，第 173 页
- *激活安全手动身份验证*，第 176 页

Websense 安全手动身份验证将使用安全套接字层 (SSL) 加密来对在客户端计算机和 Websense 软件之间传递的身份验证信息加以保护。Filtering Service 已内建一个可用来对在客户端计算机和 Filtering Service 之间传递的用户名和密码进行加密的 SSL 服务器。默认情况下，安全手动身份验证是禁用的。

注意

Remote Filtering 不能使用安全手动身份验证。在与已启动安全手动身份验证的 Filtering Service 实例相关联时，Remote Filtering Server 将无法向客户端阻止页面。

要启用此功能，您必须执行以下步骤：

1. 生成 SSL 证书和密钥，然后将它们保存至一个 Websense 软件可访问、Filtering Service 可读的位置（请参阅*生成密钥和证书*，第 175 页）。
2. 启用安全手动身份验证（请参阅*激活安全手动身份验证*，第 176 页）并对与目录服务的通讯加以保护。
3. 将证书导入浏览器（请参阅*接受客户端浏览器的证书*，第 177 页）。

生成密钥和证书

相关主题：

- *手动身份验证*，第 170 页
- *为特定的计算机设置身份验证规则*，第 173 页
- *安全手动身份验证*，第 175 页
- *激活安全手动身份验证*，第 176 页
- *接受客户端浏览器的证书*，第 177 页

证书由一个用于加密数据的公钥和一个用于解密数据的私钥组成，由 Certificate Authority (CA) 所颁发。您可以使用内部的证书服务器来生成证书，也可以从第三方 CA（例如 VeriSign）处获得一个客户端证书。

颁发客户端证书的 CA 必须受 Websense 软件信任。通常而言，这将由浏览器的设置来决定。

- 对与私钥、CSR 和证书的常见问题的解答，请参阅 httpd.apache.org/docs/2.2/ssl/ssl_faq.html#aboutcerts。
- 要了解更多关于生成私钥、 CSR 和证书的信息，请参阅 www.akadia.com/services/ssh_test_certificate.html。

可以用来生成自签名证书的工具有很多，例如：OpenSSL 工具包 （可从 www.openssl.org 获得）。

不论选择哪种证书生成方式，都可使用以下的通用步骤：

1. 生成私钥 (**server.key**)。
2. 用私钥生成证书签名申请 (CSR)。

   重要
   在提示输入 CommonName 时，输入 Filtering Server 所在计算机的 IP 地址。如跳过此步骤，则客户端浏览器将显示安全证书错误。

3. 使用 CSR 来创建自签名证书 (**server.crt**)。
4. 将 **server.crt** 和 **server.key** 文件保存至一个 Websense 软件可访问且 Filtering Service 可读的位置。

激活安全手动身份验证

相关主题：
- *手动身份验证*，第 170 页
- *为特定的计算机设置身份验证规则*，第 173 页
- *安全手动身份验证*，第 175 页
- *生成密钥和证书*，第 175 页
- *接受客户端浏览器的证书*，第 177 页

1. 停止 Websense Filtering Service（请参阅*停止和启动 Websense 服务*，第 238 页）。
2. 打开 Filtering Service 所在计算机上的 Websense 安装目录 （默认为 **C:\Program Files\Websense\bin** 或 **/opt/Websense/bin/**）。
3. 找到 **eimserver.ini**，将其备份至另一个目录。
4. 用文本编辑器打开源 INI 文件。
5. 找到 **[WebsenseServer]** 部分，然后添加如下行：

   ```
   SSLManualAuth=on
   ```

6. 在该行之下，添加如下行：

   ```
   SSLCertFileLoc=[ 路径 ]
   ```

   用 SSL 证书的全路径（包括证书文件的名称，例如 C:\secmanauth\server.crt）来替换 **[路径]**。

7. 并添加：

   ```
   SSLKeyFileLoc=[ 路径 ]
   ```

   用 SSL 密钥的全路径（包括密钥文件的名称，例如 C:\secmanauth\server.key）来替换 **[路径]**。

8. 保存并关闭 **eimserver.ini**。
9. 启动 Websense Filtering Service。

启动后，Filtering Service 将对来自默认安全 HTTP 端口 (**15872**) 的请求进行侦听。

以上步骤将确保客户端计算机和 Websense 软件之间的通讯安全无碍。要确保 Websense 软件与目录服务之间的通讯安全，请选中**设置 > 目录服务**页面上的**使用 SSL**。有关详细信息，请参阅*高级目录设置*, 第 57 页。

接受客户端浏览器的证书

相关主题：

- *手动身份验证*，第 170 页
- *为特定的计算机设置身份验证规则*，第 173 页
- *安全手动身份验证*，第 175 页
- *生成密钥和证书*，第 175 页
- *激活安全手动身份验证*，第 176 页

在首次尝试浏览某网站时，浏览器将显示一条关于安全证书的警告。要避免再次见到此消息，请在证书存储区中安装该证书。

Microsoft Internet Explorer （版本 7）

1. 打开浏览器并访问某个网站。

   出现该站点的安全证书有问题的警告。

2. 单击**继续浏览此站点 （不推荐）**。

   如收到身份验证提示，请单击**取消**。

3. 单击地址栏 （位于浏览器窗口的顶部）右侧的**证书错误**框，然后单击**查看证书**。
4. 在证书对话框的 “常规” 选项卡上，单击**安装证书**。
5. 选择**根据证书类型，自动选择证书存储区**，然后单击**下一步**。
6. 单击**完成**。

7. 在被问及是否安装该证书时，单击**是**。

然后用户在该计算机上将不会再收到与 Filtering Service 相关的证书安全警告。

Mozilla Firefox （版本 2.x）

1. 打开浏览器并访问某个网站。

   出现警告消息。
2. 单击**始终接受该证书**。
3. 在被提示时，输入您的凭据。
4. 转至**工具 > 选项**，然后单击**高级**。
5. 选择**加密**选项卡，然后单击**查看证书**。
6. 选择**网站**选项卡，并确认证书已在列表中。

然后用户在该计算机上将不会再收到与 Filtering Service 相关的证书安全警告。

Mozilla Firefox （版本 3.x）

1. 打开浏览器并访问某个网站。

   出现警告消息。
2. 单击**或者您可以添加一项例外**。
3. 单击**添加例外**。
4. 确保**始终存储此例外已选中**，然后单击**确认安全例外**。

然后用户在该计算机上将不会再收到与 Filtering Service 相关的证书安全警告。

DC Agent

相关主题：

- *透明标识*，第 169 页
- *配置 DC Agent*，第 179 页
- *为代理实例配置不同的设置*，第 193 页

Websense DC Agent 可运行在 Windows 上，并且可检测到运行 NetBIOS、WINS 或 DNS 网络服务的 Windows 网络中的用户。

DC Agent 和 User Service 将收集网络用户数据，并将其发送至 Websense Filtering Service。数据传送的速度将由多个变量共同决定，包括网络的规模以及当前网络流量的情况。

要启用 DC Agent 透明标识：

1. 安装 DC Agent 更多信息，请参阅*安装指南*中的*单个安装 Websense 组件*。

> **注意**
> 以域管理员权限运行 DC Agent。该域管理员账户必须也是 DC Agent 计算机上管理员组的成员。
>
> 为使 DC Agent 能向域控制器检索用户的登录信息，这一点是必须的。如不能以此权限来安装 DC Agent，则需在安装完成后再为这些服务配置管理员权限。更多信息，请参阅 *Websense 软件没有应用用户策略或组策略*，第 307 页。

2. 对 DC Agent 进行配置，使之能与其他 Websense 组件及网络中的域控制器通讯 （请参阅*配置 DC Agent*）。
3. 使用 Websense Manager 来添加要过滤的用户和组 （请参阅*添加客户端*，第 59 页）。

当 DC Agent 无法对用户进行透明识别时，Websense 软件将提示用户输入标识。更多信息，请参阅*手动身份验证*，第 170 页。

配置 DC Agent

相关主题：

- *透明标识*
- *手动身份验证*
- *配置用户标识方式*
- *DC Agent*
- *配置多个代理*

设置 > 用户标识 > DC Agent 页面不仅可用于新 DC Agent 实例的配置，还可用来配置适用所有 DC Agent 实例的全局设置。

要添加一个新的 DC Agent 实例，首先应提供与代理的安装位置，及 Filtering Service 将如何与之通讯相关的基本信息。这些设置对各代理实例而言可能是唯一的。

1. 在“基本代理配置”中，输入将在其上安装代理之**服务器**的 IP 地址或名称。

> **注意**
> 机器名必须以字母 (a-z) 而不是数字或特殊字符为开头。
>
> 包括某些扩展 ASCII 字符的计算机名可能无法正确解析。如果您使用的是非英语版本的 Websense 软件，则请输入 IP 地址而不是机器名。

2. 输入 DC Agent 将用来与其他 Websense 组件通讯的**端口**。默认值为 30600。
3. 要在 Filtering Service 和 DC Agent 之间建立经过身份验证的连接，请选中**启用身份验证**，然后为连接输入一个**密码**。

然后，对 DC Agent 通讯与故障排除、域控制器轮询及计算机轮询等全局设置进行配置。默认情况下，您在此进行的改动将影响所有 DC Agent 实例。但标记以星号 (*) 的设置可被代理的配置文件所重置，以能对该代理实例的行为进行自定义 （请参阅*为代理实例配置不同的设置*，第 193 页）。

1. 在 “DC Agent 通讯”中，输入 DC Agent 与其他 Websense 组件间进行通讯时将使用的**通讯端口**。默认值为 30600。

   除非应 Websense 技术支持的要求，否则请勿对**诊断端口**设置进行任何更改。默认值为 30601。
2. 在 “域控制器轮询”中，选中**启用域控制器轮询**可将 DC Agent 配置为向域控制器查询用户登录会话。

   您可以在代理的配置文件中指定各 DC Agent 实例应向哪台域控制器进行轮询。有关详细信息，请参阅*配置多个代理*, 第 192 页。
3. 使用**查询间隔**字段可指定 DC Agent 向域控制器进行查询的频率（以秒计）。

   减小查询间隔可令对登录会话的捕捉更准确，但也会加大整个网络的流量；加大查询间隔可减少网络流量，但也会导致对某些登录会话的捕捉被延迟或阻止。默认设置为 10 秒钟。
4. **用户输入超时**字段可用来指定 DC Agent 对其映射中的用户输入进行刷新的频率 （以小时计）。默认设置为 24 小时。
5. 在 “计算机轮询”中，选中**启用计算机轮询**可将 DC Agent 配置为向计算机查询用户登录会话。从而可将在已被代理纳入查询范围中的域以外的计算机也包括在内。

   DC Agent 将使用 WMI (Windows Management Instruction) 来进行计算机轮询。如已启用计算机轮询，则请将客户端计算机的 Windows Firewall 配置为允许端口 **135** 上的通讯。
6. 输入**用户映射验证间隔**可指定 DC Agent 与客户端计算机联系以对登录用户进行验证的频率。默认设置为 15 分钟。

   DC Agent 会将查询结果与其发送至 Filtering Service 的用户映射中的用户名 /IP 地址二元组进行比较。减小此间隔可提高用户映射的准确性，但会加大网络流量；加大间隔可减少网络流量，但也可能会降低准确性。
7. 输入**用户输入超时**时间可指定 DC Agent 对其用户映射中通过计算机轮询获得的输入进行刷新的频率。默认设置为 1 小时。

   DC Agent 将删除所有在此超时时间之前的用户名 /IP 地址，且该 DC Agent 将不会被验证为当前已登录。加大此间隔可能会降低映射的准确性，因为映射可能会将老用户名保存更长的时间。

   注意

   请勿将用户输入超时间隔设置得比用户映射验证间隔还短。因为这可能会导致用户名在获得验证之前就已被删除出用户映射。
8. 单击**确定**立即保存和应用您的更改。

Logon Agent

相关主题：

- *透明标识*，第 169 页
- *配置 Logon Agent*，第 181 页
- *为代理实例配置不同的设置*，第 193 页

Websense Logon Agent 会在用户登录域时对其进行实时识别。它将消除因查询间隔问题而导致用户登录丢失的可能性。

Logon Agent （或称 Authentication Server）既可驻留在 Windows 计算机也可驻留在 Linux 计算机上。该代理可与客户端计算机上的 Websense Logon Application (LogonApp.exe) 协同工作，在用户登录 Windows 域时对他们进行识别。

大多数情况下，使用 DC Agent 或 Logon Agent 之一便已足够，但您也可以同时使用这两种代理。这种情况下， Logon Agent 将具有相对 DC Agent 的优先权。DC Agent 只在 Logon Agent 可能遗漏某个登录会话 （不大可能发生）时才会就该登录会话与 Filtering Service 进行通讯。

安装 Logon Age，然后从某一中心位置将 Logon Application 部署至客户端计算机。更多信息，请参阅 *安装指南*。

完成安装后，对代理进行配置以与客户端计算机和 Websense Filtering Service 进行通讯 （请参阅 *配置 Logon Agent*）。

注意

如果您使用的是 Windows Active Directory（本地模式）且安装在一台 Linux 计算机上，则请参阅 *在 Linux 上运行的 User Service*, 第 313 页以了解其他配置步骤。

配置 Logon Agent

相关主题：

- *透明标识*，第 169 页
- *手动身份验证*，第 170 页
- *配置用户标识方式*，第 171 页
- *Logon Agent*，第 181 页
- *配置多个代理*，第 192 页

设置 > 用户标识 > Logon Agent 页面不仅可用于新 Logon Agent 实例的配置，还可用来配置适用所有 Logon Agent 实例的全局设置。

要添加一个新的 Logon Agent 实例：

1. 在“基本代理配置”中，输入将在其上安装代理之**服务器**的 IP 地址或名称。

   注意
   机器名必须以字母 (a-z) 而不是数字或特殊字符为开头。

   包括某些扩展 ASCII 字符的计算机名可能无法正确解析。如果您使用的是非英语版本的 Websense 软件，则请输入 IP 地址而不是机器名。

2. 输入 Logon Agent 将用来与其他 Websense 组件通讯的**端口**。默认值为 30602。
3. 要在 Filtering Service 和 Logon Agent 之间建立经过身份验证的连接，请选中**启用身份验证**，然后为连接输入一个**密码**。
4. 单击**确定**以保存您的更改，或继续页面的下一部分以输入其他配置信息。

然后，对全局 Logon Agent 通讯设置进行自定义配置。默认情况下，您在此进行的改动将影响所有 Logon Agent 实例。

1. 在“Logon Agent 通讯”中，输入 Logon Agent 与其他 Websense 组件间进行通讯时将使用的**通讯端口**。默认值为 30602。
2. 除非应 Websense 技术支持的要求，否则请勿对**诊断端口**设置进行任何更改。默认值为 30603。
3. 在“Logon Application 通讯”中，指定登录应用程序用来与 Logon Agent 进行通讯的**连接端口**。默认值为 15880。
4. 输入各 Logon Agent 实例所允许的**最大连接数**。默认值为 200。

   如网络规模较大，则需加大此数值。但加大该数值将加大网络流量。
5. 单击**确定**以保存您的更改，或继续页面的下一部分以输入其他配置信息。

在对将确定用户输入有效性的决定方式的默认设置进行配置之前，您必须先确定 Logon Agent 和客户端登录应用程序的工作方式是**持续模式**还是**非持续模式**（默认）。

非持续模式可通过在启动 **LogonApp.exe** 时包含 /NOPERSIST 参数来激活（更多信息请参阅 **LogonApp_ReadMe.txt** 文件，该文件将包括在 Logon Agent 安装包内）。

- 在持续模式下，登录应用程序将定期地与 Logon Agent 就用户的登录信息进行通讯。

  如使用持续模式，则请指定**查询间隔**，以确定登录应用程序就登录信息进行通讯的频率。

  注意
  对此值的更改将在前一间隔期结束后生效。例如，假设您将间隔从 15 分钟更改为 5 分钟，则每 5 分钟一次的查询在当前的 15 分钟间隔结束后才会开始。

- 在非持续模式下，登录应用程序每次登录都会向 Logon Agent 发送一次登录信息。

  如果使用的是非持续模式，则请指定**用户输入过期**的时间段。在此超时时间结束后，用户输入将自用户映射中删除。

在完成配置更改后，请单击**确定**以保存您的设置。

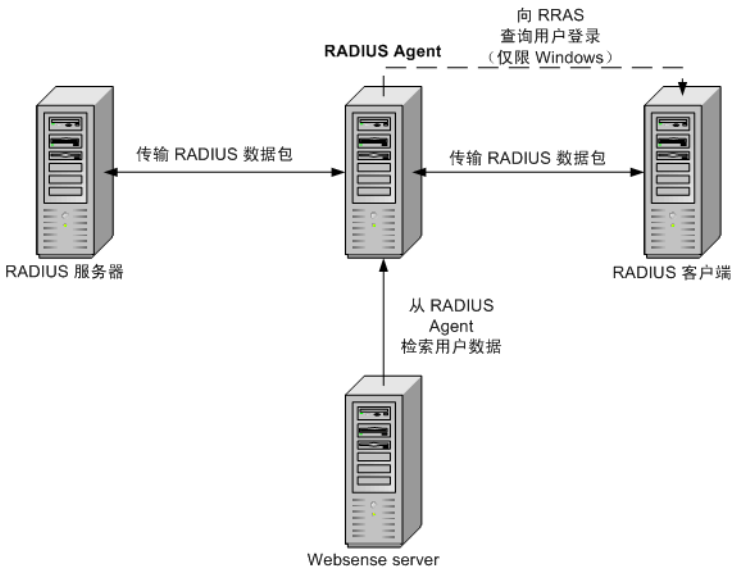
RADIUS Agent

相关主题：

- *透明标识*，第 169 页
- *处理 RADIUS 流量*，第 184 页
- *配置 RADIUS 环境*，第 184 页
- *配置 RADIUS 代理*，第 185 页
- *配置 RADIUS 客户端*，第 186 页
- *配置 RADIUS 服务器*，第 187 页
- *为代理实例配置不同的设置*，第 193 页

Websense RADIUS Agent 将使您能通过由 RADIUS server 提供的身份验证来应用基于用户和组的策略。RADIUS Agent 支持对通过拨号、私有专用网 (VPN)、数字用户线 (DSL) 或其他远程连接 （取决于您的配置）来访问贵网络的用户进行透明标识。

RADIUS Agent 将与网络中的 RADIUS 服务器和 RADIUS 客户端一起，对远程访问拨号用户服务 (RADIUS) 协议流量进行处理和追踪。从而使您为通过远程方式来访问网络的用户和组以及本地用户指定特定的筛选策略。



在安装时 RADIUS Agent， Agent 可与现有的 Websense 组件相集成。但前提是 RADIUS Agent、RADIUS 服务器和 RADIUS 客户端都必须进行适当地配置（请参阅*配置 RADIUS 代理*，第 185 页）。

处理 RADIUS 流量

Websense RADIUS Agent 可作为在一台或多台 RADIUS 客户端和 RADIUS 服务器之间进行 RADIUS 消息转发的代理。

RADIUS Agent 不会直接对用户进行身份验证。相反，该代理将对远程用户进行识别，并将他们与 IP 地址相关联，以便 RADIUS 服务器对这些用户进行身份验证。理想情况下， RADIUS 服务器会将身份验证请求转发给某项基于 LDAP 的目录服务。

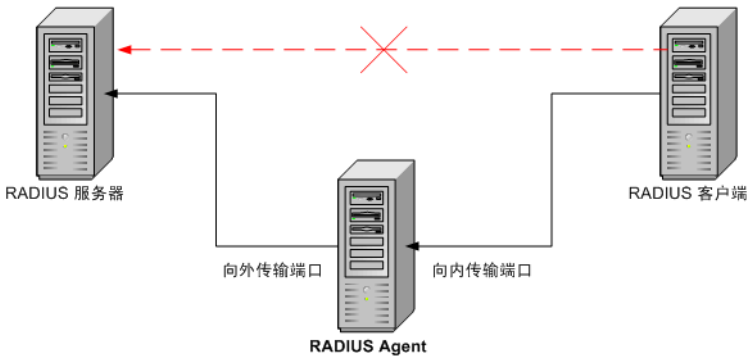
RADIUS Agent 将把用户名、 IP 地址二元组保存在用户映射中。如果您的 RADIUS 客户端支持并已启用记帐（或用户登录跟踪），则 RADIUS Agent 将可以从其所收到的 RADIUS 消息中收集到更多与用户登录会话相关的详细信息。

配置得当时， Websense RADIUS Agent 可捕获和处理所有以下类型的 RADIUS 协议包：

- **访问请求**：由 RADIUS 客户端发出、针对网络访问连接尝试的身份验证申请。
- **访问接受**：由 RADIUS 服务器发出、对访问请求消息的回应，它将告知 RADIUS 客户端连接尝试已获授权并已通过身份验证。
- **访问拒绝**：由 RADIUS 服务器发出、对访问请求消息的回应，它将告知 RADIUS 客户端连接尝试已被拒绝。
- **记帐暂停请求**：由 RADIUS 客户端发出，旨在告知 RADIUS 服务器停止对用户活动进行追踪。

配置 RADIUS 环境

Websense RADIUS Agent 可作为 RADIUS 客户端和 RADIUS 服务器之间的代理。此图表简要地显示了使用 RADIUS Agent 与标准 RADIUS 设置之间的不同。



RADIUS Agent 和 RADIUS 服务器应安装在不同的计算机上。代理和服务器不得具有相同的 IP 地址，并必须使用不同的端口。

完成 RADIUS Agent 的安装后，请在 Websense Manager 中对之进行配置 （请参阅 *配置 RADIUS 代理*，第 185 页）。此外，您还必须：

- 将 RADIUS 客户端 （通常是网络接入服务器 [NAS]）配置为与 RADIUS Agent 进行通讯，而不是直接与 RADIUS 服务器进行通讯。
- 将 RADIUS 服务器配置为使用 RADIUS Agent 作为代理（请参阅RADIUS 服务器的文档）。如果您有多台 RADIUS 服务器，请逐一进行配置。

> **注意**
>
> 如果您使用的是 Lucent RADIUS Server 和 RRAS，则您必须将 RADIUS 服务器配置为使用密码验证协议 (PAP)，且 RRAS 服务器只接受 PAP 请求。更多信息，请参阅相关的产品文档。

配置 RADIUS 代理

相关主题：

- *透明标识*，第 169 页
- *手动身份验证*，第 170 页
- *配置用户标识方式*，第 171 页
- *RADIUS Agent*，第 183 页
- *配置多个代理*，第 192 页

使用**设置 > 用户标识 > RADIUS Agent** 页面不仅可配置新的 RADIUS Agent 实例，还可配置适用于所有 RADIUS Agent 实例的全局设置。

要添加一个新的 RADIUS Agent 实例：

1. 在“基本代理配置”中，输入将在其上安装代理之**服务器**的 IP 地址或名称。

   > **注意**
   >
   > 计算机名必须以字母 (a-z) 而不是数字或特殊字符为开头。
   >
   > 包括某些扩展 ASCII 字符的计算机名可能无法正确解析。如果您使用的是非英语版本的 Websense 软件，则请输入 IP 地址而不是机器名。

2. 输入 RADIUS Agent 将用来与其他 Websense 组件通讯的**端口**。默认值为 30800。
3. 要在 Filtering Service 和 RADIUS Agent 之间建立经过身份验证的连接，请选中**启用身份验证**，然后为连接输入一个**密码**。
4. 单击**确定**以保存您的更改，或继续页面的下一部分以输入其他配置信息。

然后，对全局 RADIUS Agent 通讯设置进行自定义配置。默认情况下，您在此进行的改动将影响所有 RADIUS Agent 实例。但标记以星号 (*) 的设置可被代理的配置文件所重置，以能对该代理实例的行为进行自定义 （请参阅*为代理实例配置不同的设置，第 193 页*）。

1. 输入在 RADIUS Agent 和其他 Websense 组件之间进行通讯将使用的**通讯端口**。默认值为 30800。
2. 除非应 Websense 技术支持的要求，否则请勿对**诊断端口**设置进行任何更改。默认值为 30801。
3. 在“RADIUS Server”中，输入 **RADIUS 服务器 IP 或名称**。RADIUS Agent 将把身份验证请求转发至 RADIUS 服务器，并必须知悉该计算机的标识。
4. 如使用的是 Microsoft RRAS，则请输入 **RRAS 计算机**的 IP 地址。Websense 软件将向此计算机查询用户的登录会话。
5. 请输入用于确定 RADIUS Agent 用户映射刷新频率的**用户输入超时**间隔。通常而言，默认查询时间间隔 （24 小时）即为最佳选择。
6. 使用**身份验证端口**和**记帐端口**可指定 RADIUS Agent 将使用什么端口来发送及接收身份验证和记帐请求。对各种通讯类型，您可指定以下之间的通讯应使用什么端口：
   - RADIUS Agent 与 RADIUS 服务器
   - RADIUS Agent 与 RADIUS 客户端
7. 在完成后，请单击**确定**以立即保存您的设置。

配置 RADIUS 客户端

您的 RADIUS 客户端必须被配置为通过 RADIUS Agent 来向 RADIUS 服务器传送身份验证和记帐请求。

修改您的 RADIUS 客户端，以：

- RADIUS 客户端将身份验证请求发送至 RADIUS Agent 侦听身份验证请求的计算机和端口。该**身份验证端口**应于 RADIUS Agent 配置期间指定。
- RADIUS 客户端将记帐请求发送至 RADIUS Agent 侦听记帐请求的计算机和端口。该**记帐端口**应于 RADIUS Agent 配置期间指定。

RADIUS 客户端的具体配置程序将因客户端的类型而不尽相同。详细信息，请参阅您的 RADIUS 客户端文档。

注意

在所发送的身份验证和记帐消息中， RADIUS 客户端应将**用户名**和**分段 IP 地址**属性包括在内。 RADIUS Agent 将使用这些属性的值来解析和存储用户名 /IP 地址二元组。如果您的 RADIUS 客户端不能按默认生成这些信息，则需配置以进行此操作 （请参阅 RADIUS 客户端文档）。

配置 RADIUS 服务器

要令 Websense RADIUS Agent 能正确地与您的 RADIUS 服务器进行通讯：

- 将 RADIUS Agent 计算机的 IP 地址添加至 RADIUS 服务器的客户端列表。详细说明，请参阅您的 RADIUS 服务器文档。
- 在 RADIUS 服务器和所有使用该代理来与服务器通讯的 RADIUS 客户端之间定义共享密钥。其中，共享密钥通常都被指定为身份验证安全选项。

  为 RADIUS 客户端和 RADIUS 服务器配置一个共享密钥将使 RADIUS 消息的传递能够保密进行。共享密钥通常是一个常见的文本字符串。详细说明，请参阅您的 RADIUS 服务器文档。

> **注意**
>
> 在身份验证和记帐消息中，RADIUS 服务器应将**用户名**和**分段 IP 地址**属性包括在内。RADIUS Agent 将使用这些属性的值来解析和存储用户名 /IP 地址二元组。如果您的 RADIUS 服务器不能按默认生成这些信息，则需配置以进行此操作 （请参阅 RADIUS 服务器文档）。

eDirectory Agent

相关主题：

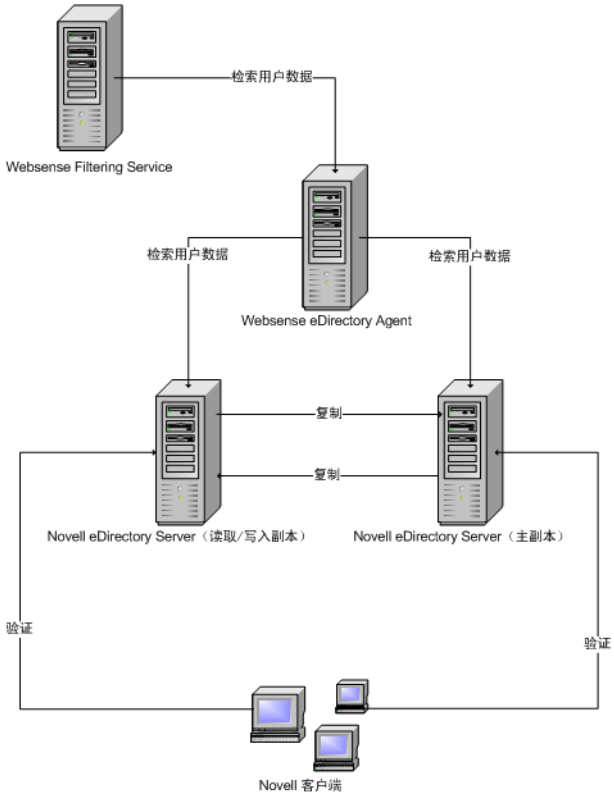
- *透明标识*，第 169 页
- *配置 eDirectory Agent*，第 189 页
- *为代理实例配置不同的设置*，第 193 页

Websense eDirectory Agent 可与 Novell eDirectory 协作来透明识别用户，从而令 Websense 软件能按为用户、组、域或组织机构分配的策略来对用户进行筛选。

eDirectory Agent 可向 Novell eDirectory 收集用户的登录会话信息，而后者可对登录网络的用户进行身份验证。然后代理将把各个已通过身份验证的用户与 IP 地址相关联，并将用户名与 IP 地址的二元组记录入本地的用户映射。然后由 eDirectory Agent 就此信息与 Filtering Service 进行通讯。

> **注意**
>
> 从运行 Windows 的 Novell 客户端，多位用户可同时登录同一台 Novell eDirectory 服务器。这将使同一 IP 地址同时与多位用户相关联。在这种情况下，的用户映射将只保存从给定地址登录的用户中最后一位的用户名 /IP 地址二元组。

一个 Websense eDirectory Agent 可以支持一个 Novell eDirectory 主机，外加任何数量的 Novell eDirectory 副本。



特殊配置考虑

- 如已为 Websense 软件集成 Cisco Content Engine v5.3.1.5 或以上版本：
  - 在与 Cisco Content Engine 相同的计算机上运行以下 Websense 服务：

    Websense eDirectory Agent
    Websense User Service
    Websense Filtering Service
    Websense Policy Server
  - 确保所有的 Novell eDirectory 副本都已添加至同一计算机上的 **wsedir.ini** 文件中。
  - 删除 **eDirAgent.bak** 文件。

  在 Cisco Content Engine 与和 Websense 软件**不同**的计算机上运行 Websense Reporting Tools 服务。
- Websense 软件支持 NMAS 与 eDirectory Agent 配合使用。要在启用 NMAS 的情况下使用 eDirectory Agent，eDirectory Agent 必须安装在同时运行 Novell Client 的计算机上。

配置 eDirectory Agent

相关主题：

- *透明标识*，第 169 页
- *手动身份验证*，第 170 页
- *配置用户标识方式*，第 171 页
- *eDirectory Agent*，第 187 页
- *将 eDirectory Agent 配置为使用 LDAP*，第 191 页
- *配置多个代理*，第 192 页

使用**设置 > 用户标识 > eDirectory Agent** 页面不仅可配置新的 eDirectory Agent 实例，还可配置适用于所有 eDirectory Agent 实例的全局设置。

要添加一个新的 eDirectory Agent 实例：

1. 在“基本代理配置”中，输入将在其上安装代理之**服务器**的 IP 地址或名称。

   注意

   机器名必须以字母 (a-z) 而不是数字或特殊字符为开头。

   包括某些扩展 ASCII 字符的计算机名可能无法正确解析。如果您使用的是非英语版本的 Websense 软件，则请输入 IP 地址而不是机器名。

2. 输入 eDirectory Agent 将用来与其他 Websense 组件通讯的**端口**。默认值为 30700。
3. 要在 Filtering Service 和 eDirectory Agent 之间建立经过身份验证的连接，请选中**启用身份验证**，然后为连接输入一个**密码**。
4. 单击**确定**以保存您的更改，或继续页面的下一部分以输入其他配置信息。

然后，对全局 eDirectory Agent 通讯设置进行自定义配置。默认情况下，您在此进行的改动将影响所有 eDirectory Agent 实例。但标记以星号 (*) 的设置可被代理的配置文件所重置，以能对该代理实例的行为进行自定义（请参阅*为代理实例配置不同的设置*，第 193 页）。

1. 输入在 eDirectory Agent 和其他 Websense 组件之间进行通讯将使用的**通讯端口**。默认值为 30700。
2. 除非应 Websense 技术支持的要求，否则请勿对**诊断端口**设置进行任何更改。默认值为 30701。
3. 在 eDirectory Server 中指定**搜索库**（根上下文），以供 eDirectory Server 用作在目录中搜索用户时的起始点。

4. 提供 eDirectory Agent 用于目录通讯的管理用户账户信息：
   a. 输入 Novell eDirectory 管理用户账户的**管理员可分辨名称**。
   b. 输入该账户的**密码**。
   c. 指定**用户输入超时**间隔，以指明输入项在代理的用户映射中的保留时长。

      此间隔应比通常的用户登录会话长 30%，以有助于防止用户输入在用户结束浏览之前就已被自映射中删除。

      通常而言，默认时间间隔 （24 小时）即为推荐设置。

      注意
      在某些环境下，可不通过用户输入超时间隔来决定 eDirectory Agent 对其用户映射进行更新的频率，而是按一定间隔地来向 eDirectory Server 查询用户登录的更新情况。请参阅*启用完整 eDirectory Server 查询*，第 191 页。

5. 将 eDirectory Server 主机及所有副本添加至 **eDirectory Replicas** 列表。要将 eDirectory Server master 主机或副本添加至该列表，请单击**添加**，然后按*添加 eDirectory 服务器副本*，第 190 页中的说明执行。

在完成配置更改后，请单击**确定**以保存您的设置。

添加 eDirectory 服务器副本

一个 Websense eDirectory Agent 可以支持一个 Novell eDirectory 主机，外加运行在独立计算机上的任何数量的 Novell eDirectory 副本。

eDirectory Agent 必须能与运行目录服务器副本的各台计算机进行通讯。这将确保代理能以最快的速度获得最新的登录信息，并无需等待 eDirectory 复制的完成。

Novell eDirectory 会每 5 分钟对能唯一识别已登录用户端属性进行一次复制。而 eDirectory Agent 可在用户登录任何 eDirectory 副本后迅速捕获这些新的登录会话，不受这些同步延时的任何影响。

要将所安装的 eDirectory Agent 配置为可与 eDirectory 进行通讯：

1. 在 “添加 eDirectory 副本” 页面中，输入 eDirectory **Server** （主机或副本）的 IP 地址或名称。
2. 输入 eDirectory Agent 将用来与 eDirectory 计算机通讯的**端口**。
3. 单击**确定**以返回 eDirectory 页面。然后新项将显示在 eDirectory Replicas 列表中。
4. 对所有其他的 eDirectory 服务器计算机重复该流程。
5. 单击**确定**以缓存更改，然后单击**全部保存**。
6. 停止并启动 eDirectory Agent，以便代理能开始与新的副本进行通讯。请参阅*停止和启动 Websense 服务*, 第 238 页以了解相关说明。

将 eDirectory Agent 配置为使用 LDAP

Websense eDirectory Agent 可使用网络核心协议 (NCP) 或轻量目录访问协议 (LDAP) 从 Novell eDirectory 获得用户登录信息。默认情况下，Windows 平台的 eDirectory Agent 将使用 NCP。而 Linux 平台的 eDirectory Agent 将使用 LDAP。

如果您运行的是 Windows 平台的 eDirectory Agent，而又想使用 LDAP 来查询 Novell eDirectory，则请将代理设置为使用 LDAP 而不是 NCP。一般而言，NCP 所提供的查询机制效率更高。

要将 Windows 平台的 eDirectory Agent 设置为使用 LDAP：

1. 确保至少有一个 Novell eDirectory 副本包含对整个网络进行监控和筛选所需的全部目录对象。
2. 停止 Websense eDirectory Agent 服务 （请参阅 *停止和启动 Websense 服务*，第 238 页）。
3. 转至 eDirectory Agent 安装目录 （默认为 **\Program Files\Websense\bin**），然后用文本编辑器打开 **wsedir.ini** 文件。
4. 按如下方式更改 **QueryMethod** 项：

   ```
   QueryMethod=0
   ```

   这将把代理设置为使用 LDAP 来查询 Novell eDirectory （默认值为 1，即使用 NCP）。
5. 保存并关闭文件。
6. 重新启动 Websense eDirectory Agent 服务。

启用完整 eDirectory Server 查询

对小型网络，您可将 Websense eDirectory Agent 配置为按固定间隔向 eDirectory Server 查询所有的已登录用户。这将使代理能在侦测新登录用户和上次查询后已注销用户的同时，相应地对本地的用户映射进行更新。

重要

对大型网络，不推荐将 eDirectory Agent 配置为使用完整查询，因为返回查询结果所需的时间长短将取决于已登录用户的数量。已登录的用户越多，对性能的影响就越大。

在为 eDirectory Agent 启用完整查询后，**用户输入超时**间隔将被忽略，因为已注销的用户将通过查询来识别。默认情况下，该查询将每 30 秒进行一次。

启用此功能将在两个方面增加 eDirectory Agent 的处理时间：

- 每次进行查询时，对已登录用户的名称进行检索所需的时间。
- 处理用户名称信息、从本地用户映射中删除老旧项以及根据最新的查询来添加新项所需的时间。

每次查询后， eDirectory Agent 都将对整个本地用户映射进行检查，而不是仅识别新登录的用户。此处理所需的时间将取决于每次查询所返回的用户数量。因此，查询处理将同时对 eDirectory Agent 和 Novell eDirectory Server 的响应时间产生影响。

要启用完整查询：

1. 在 eDirectory Agent 计算机上，转至 Websense 的 **bin** 目录 （默认为 C:\Program Files\Websense\bin or /opt/Websense/bin）。
2. 找到 **wsedir.ini** 文件，将其备份至另一个目录。
3. 用文本编辑器 （如记事本或 vi）打开 **wsedir.ini**。
4. 转至文件中的 **[eDirAgent]** 部分并找到如下项：

   ```
   QueryMethod=<N>
   ```

   记下 QueryMethod 的值，以供您在今后将其改回默认设置时使用。
5. 按如下方式更新 **QueryMethod** 的值：
   - 如当前值为 0 （通过 LDAP 来与目录通讯），请将其更改为 **2**。
   - 如当前值为 1 （通过 NCP 来与目录通讯），请将其更改为 **3**。

   注意
   如对此查询值的更改降低了系统的性能，则请将 QueryMethod 项改回其之前的值。
6. 如默认查询间隔 （30 秒）不适用于您的环境，则请相应地编辑 **PollInterval** 的值。

   请注意该间隔时间以**微秒**计。
7. 保存并关闭文件。
8. 重新启动 Websense eDirectory Agent 服务 （请参阅*停止和启动 Websense 服务*，第 238 页）。

配置多个代理

相关主题：
- *DC Agent*，第 178 页
- *Logon Agent*，第 181 页
- *RADIUS Agent*，第 183 页
- *eDirectory Agent*，第 187 页

在同一网络内配置多个透明标识代理是可以的。如果您的网络配置需要多个代理，则最好将各个代理安装在不同的计算机上。但在某些情况下，您也可以将 Websense 软件配置为与同一计算机上的多个代理协同工作。

所支持的透明标识代理组合如下：

组合	同一计算机？	同一网络？	需要配置
多个 DC Agent	否	是	确保所有的 DC Agent 实例都能与 Filtering Service 进行通讯。
多个 RADIUS Agent	否	是	将每个代理都配置为能与 Filtering Service 进行通讯。
多个 eDirectory Agent	否	是	将每个代理都配置为能与 Filtering Service 进行通讯。
多个 Logon Agent	否	是	将每个代理都配置为能与 Filtering Service 进行通讯。
DC Agent + RADIUS Agent	是	是	这些代理应安装在不同的目录下。将各个代理配置为使用不同的通讯端口来与 Filtering Service 进行通讯。
DC Agent + eDirectory Agent	否	否	Websense 软件不支持同一部署同时与 Windows 和 Novell 目录服务通讯。但您可同时安装两个代理，并只激活其中之一。
DC Agent + Logon Agent	是	是	将两个代理都配置为能与 Filtering Service 进行通讯。默认情况下，各个代理都会使用唯一的端口，因此在未对这些端口进行更改之前，不会出现端口冲突的问题。
eDirectory Agent + Logon Agent	否	否	Websense 软件不支持同一部署同时与 Windows 和 Novell 目录服务通讯。但您可同时安装两个代理，并只激活其中之一。
RADIUS Agent + eDirectory Agent	是	是	将各个代理配置为使用不同的通讯端口来与 Filtering Service 进行通讯。
DC Agent + Logon Agent + RADIUS Agent	是	是	虽然此组合很少有需要，但受到支持。 将各个代理安装在不同的目录中。并将各个代理配置为使用不同的通讯端口来与 Filtering Service 进行通讯。

为代理实例配置不同的设置

Websense Manager 透明标识代理配置设置是全局设置，适用于已安装的全部代理实例。但对任一代理的多个实例，您都可以独立于其他实例地单独对某个实例进行配置。

为某个特定代理实例指定的设置将替代 “设置”对话框中的全局设置。可被替代的设置将以星号 (*) 来标记。

1. 停止透明标识代理服务 （请参阅*停止和启动 Websense 服务*，第 238 页）。
2. 在运行代理实例的计算机上，转至代理的安装目录并用文本编辑器打开相应的文件：
   - 对 DC Agent：**transid.ini**
   - 对 Logon Agent：**authserver.ini**
   - 对 eDirectory Agent：**wsedir.ini**
   - 对 RADIUS Agent：**wsradius.ini**
3. 找到要为此代理实例更改的参数 （请参阅 *INI 文件参数*，第 195 页）。

   例如，您可以启用代理实例与其他 Websense 服务之间需要身份验证的连接。为此，请在 INI 文件中输入 **password** 参数的值：

   ```
   password=[xxxxxx]
   ```
4. 按需要更改所有其他的值。
5. 保存并关闭 INI 文件。
6. 如果您对 **DC Agent** 的设置进行了更改，则必须从 Websense 的 **bin** 目录（默认为 C:\Program Files\Websense\bin）下删除 2 个文件：
   a. 停止 DC Agent 计算机上的所有 Websense 服务 （请参阅*停止和启动 Websense 服务*，第 238 页）。
   b. 删除以下文件：

      ```
      Journal.dat
      XidDcAgent.bak
      ```

      这些文件将在您启动 Websense DC Agent 服务时重新创建。
   c. 重新启动 Websense 服务 （包括 DC Agent），然后跳转至**步骤 8**。
7. 停止透明标识代理服务。
8. 在 Websense Manager 中对代理设置进行更新：
   a. 转至**设置** > 用户标识。
   b. 在 **Transparent Identification Agents** 中，选择代理然后单击**编辑**。

      注意

      如果您更改了此代理实例的**端口**值，请删除然后重新添加该代理。首先选择现有的代理项并单击**删除**，然后单击**添加代理**。

   c. 请验证此代理实例所使用的**服务器 IP 或名称**及**端口**。如果您在 INI 文件中指定了唯一的端口号，则请确保您的项与该值相匹配。
   d. 如果您在 INI 文件中指定了一个唯一的身份验证密码，则请确保在此处所显示的**密码**项是正确的。
   e. 单击**确定**以缓存您的更改。直到您单击**全部保存**之后，更改才会生效实施。

INI 文件参数

Websense Manager 字段标签	.ini 参数名称	描述
通讯端口 （*所有代理*）	端口	代理用来与其他 Websense 服务进行通讯的端口。
诊断端口 （*所有代理*）	DiagServerPort	代理的故障排除工具用以侦听来自代理之数据的端口。
密码 （*所有代理*）	密码	代理用来对与其他 Websense 服务之间的连接进行身份验证的密码。请指定一个密码以启用身份验证。
查询间隔 (*DC Agent*)	QueryInterval	DC Agent 向域控制器进行查询的时间间隔。
服务器 IP 或名称 端口 (*eDirectory Agent*)	Server=IP:port	运行 eDirectory Agent 的计算机的 IP 地址和端口号。
搜索库 (*eDirectory Agent*)	SearchBase	Novell eDirectory 服务器的根上下文。
管理员可分辨名称 (*eDirectory Agent*)	DN	Novell eDirectory 服务器的管理员用户的名称。
密码 (*eDirectory Agent*)	PW	Novell eDirectory 服务器的管理员用户的密码。
RADIUS 服务器 IP 或名称	RADIUSHost	RADIUS 服务器计算机的 IP 地址或名称。
RRAS 计算机的 IP（仅限 Windows）： (*RADIUS Agent*)	RRASHost	运行 RRAS 的计算机的 IP 地址。Websense 将向此计算机查询用户的登录会话。
身份验证端口：在 RADIUS Agent 和 RADIUS 服务器之间	AuthOutPort	RADIUS 服务器用来侦听身份验证请求的端口。
身份验证端口：在 RADIUS 客户端和 RADIUS Agent 之间	AuthInPort	RADIUS Agent 用来接受身份验证请求的端口。
记帐端口：在 RADIUS Agent 和 RADIUS 服务器之间	AccOutPort	RADIUS 服务器用来侦听记帐消息的端口。
记帐端口：在 RADIUS 客户端和 RADIUS Agent 之间	AccInPort	RADIUS Agent 用来接受记帐消息的端口。

将代理配置为忽略特定的用户名

您可以将透明标识代理配置为忽略未与实际用户相关联的登录名称。该功能通常用来处理某些 Windows 200x 和 XP 服务与网络中的域控制器进行联络的方式。

例如，**user1** 在登录网络后被域控制器识别为 **computerA/user1**。该用户将由为 **user1** 指派的 Websense 策略进行筛选。如果在一台通过识别 **computerA/ServiceName** 来联系域控制器的用户计算机上启动服务，则将导致筛选出现问题。软件将把 **computerA/ServiceName** 视为尚未指定策略的新用户，因此将按计算机策略或**默认**策略来筛选此用户。

要解决此问题：

1. 停止代理服务 （请参阅*停止和启动 Websense 服务*，第 238 页）。
2. 转至 **\Websense\bin** 目录，然后用文本编辑器打开 **ignore.txt** 文件。
3. 每行输入一个用户名称。不要包括通配字符，如 “*”。

   ```
   maran01
   WindowsServiceName
   ```

   Websense 软件将忽略这些用户名，不论他们与哪些计算机相关联。

   要指示 Websense 软件忽略特定域的某个用户名，请使用格式**用户名、域**。

   ```
   aperez, engineering1
   ```
4. 完成后，保存并关闭文件。
5. 重新启动代理服务。

代理将忽略指定的用户名，且 Websense 软件在进行筛选时将不考虑这些名称。

11 委派管理

相关主题：

- *管理角色概述*，第 197 页
- *管理员概述*，第 198 页
- *从管理角色开始*，第 201 页
- *启用 Websense Manager 访问*，第 208 页
- *使用委派管理*，第 211 页
- *多个管理员访问 Websense Manager*，第 220 页
- *定义所有角色的筛选器限制*，第 221 页

委派管理提供强大而灵活的功能，可管理面向特定客户端组的 Internet 筛选和报告。在所有用户都位于中心位置时，这是一种向各个经理分配 Internet 访问管理和报告职责的高效方法。对于包括多个办公地点、涉及不同地理区域的大型组织，这种方法可允许本地管理员管理 Internet 访问并向其本地的用户报告筛选活动，因而尤为高效。

执行委派管理需要针对同一个管理员管理的每组客户端创建管理角色。每个角色中的各个管理员可被授予其客户端的管理策略权限或生成报告的权限，或者同时获授予两种权限。请参阅*从管理角色开始*，第 201 页。

超级管理员角色将预安装，它包括默认的管理员用户：WebsenseAdministrator。与其他角色中的管理员相比，超级管理员可以访问的策略和配置设置范围更加广泛。请参阅*超级管理员*，第 198 页。

管理角色概述

相关主题：

- *管理员概述*，第 198 页
- *从管理角色开始*，第 201 页

管理角色是由一个或多个管理员管理的受管理客户端集合，它包括用户、组、域、组织单位、计算机和网络范围。您可授予各个管理员将策略应用到角色的客户端或生成报告的权限，也可同时授予这两种权限。

Websense 软件提供预定义的超级管理员角色。此外，还有一个默认用户 WebsenseAdministrator，它会自动成为超级管理员角色的成员。您可将管理员添加到此角色，但不能删除此默认管理员。

重要

您不能删除预定义的超级管理员角色。默认用户 WebsenseAdministrator 是超级管理员角色中的管理员，但它不会在此角色中列出。您不能删除或更改 WebsenseAdministrator 的权限。

根据您组织的情况创建相应数量的角色。例如，您可以针对每个部门创建角色，让部门经理成为管理员，让部门成员成为受管理客户端。在分布在不同地理区域的组织内，您可以为每个地理区域创建角色并将该地区的所有用户分配为该角色的受管理客户端。然后，将该地区的一个或多个个人分配为管理员。

请参阅 *管理员概述*，第 198 页，以了解定义管理员时可用选项的有关信息。

请参阅 *使用委派管理*，第 211 页，以了解创建角色和配置权限的有关说明。

管理员概述

管理员是可以访问 Websense Manager 以针对客户端组管理策略或生成报告的个人。具体的可用权限将依角色的类型而异。

- 超级管理员是 Websense Manager 中预定义的特殊角色。该角色具有定义访问权限的最灵活方法。请参阅*超级管理员*，第 198 页。
- 委派管理角色必须由超级管理员创建。这些角色的管理员所拥有的访问权限较小。请参阅*委派管理员*，第 200 页。

此外，您可创建一些仅限报告的委派管理角色，从而让多人能够创建报告同时又不用授予他们策略管理的职责。

您可使用网络登录凭据为角色分配管理员，或者也可创建仅限访问 Websense Manager 的特殊帐户。请参阅*启用 Websense Manager 访问*，第 208 页。

超级管理员

相关主题：

- *管理员概述*，第 198 页
- *委派管理员*，第 200 页
- *多种角色中的管理员*，第 200 页

超级管理员角色是在安装过程中所创建。默认用户 WebsenseAdministrator 将被自动分配给此角色。因此，当您第一次使用安装时所设置的该用户名和密码登录时，您将获得在 Websense Manager 中访问所有策略、报告和配置设置的全部管理权限。

要保留该帐户的全部访问权限， WebsenseAdministrator 不能出现在超级管理员角色的管理员列表中。它不能删除，其权限也不能修改。

您可根据需要向超级管理员角色添加管理员。每位管理员可获得以下权限：

- **策略**权限允许超级管理员创建和编辑委派管理角色，并允许在适当时将筛选器和策略复制到这些角色。他们还可创建和编辑筛选组件、筛选器和策略，将策略应用于不受任何其他角色管理的客户端。

  此外，具有策略权限的超级管理员可查看审核日志，他们可访问 Websense 配置和其他选项，具体如下：

  - **无限制**权限使超级管理员可访问 Websense 安装时的所有系统配置设置，例如帐户、Policy Server、Remote Filtering Server 设置、风险级别分配和记录选项。

    无限制超级管理员可选择创建 “筛选器锁定”，以阻止委派管理角色所管理的所有用户访问某些类别和协议。请参阅*定义所有角色的筛选器限制*，第 221 页，以了解更多信息。

    无限制超级管理员可修改超级管理员角色，根据需要添加和删除管理员。他们也可删除委派管理角色或者从这些角色中删除管理员或客户端。

  - **受限制**权限使超级管理员能够访问数据库下载、目录服务、用户标识和 Network Agent 配置设置。也具有报告权限的受限制超级管理员可访问报告工具的配置设置。

    受限制超级管理员可添加 Websense 用户帐户，但不能删除它们。他们可创建和编辑委派管理角色，但不能删除角色，或分配给他们的管理员或受管理客户端。他们也不能从超级管理员角色中删除管理员。

- **报告**权限使超级管理员能够访问所有报告功能和关于所有用户的报告。无限制超级管理员可自动获得报告权限。

  如果管理员仅获得报告权限，则不可使用 “常见任务”列表中的 “创建策略”、“重新分类 URL”和 “取消阻止 URL”选项。此外，工具箱中的 “查看策略”选项也不可用。

创建多个无限制超级管理员可确保当主要超级管理员不在时，其他管理员仍能访问所有的 Websense 策略和配置设置。

请记住：2 个管理员不能同时登录管理同一个角色的策略。请参阅*多个管理员访问 Websense Manager*，第 220 页，以了解如何避免冲突的更多信息。

超级管理员角色的独特权限使该角色中的管理员可访问所有角色。要在登录后切换到另一个角色，请转到横幅窗格中的**角色**下拉列表，然后选择一个角色。

更改角色后，您的策略权限将限制为委派管理角色可用的权限。您创建的筛选器和策略仅供该角色中的管理员使用。它们只能应用于该角色中的受管理客户端。请参阅*委派管理员*，第 200 页。

报告权限具有累积性，这意味着您可以获得以管理员身份参与的所有角色的综合权限。无限制超级管理员享有全部报告权限，而无论他们访问哪一种角色。

委派管理员

相关主题：

- *管理员概述*，第 198 页
- *超级管理员*，第 198 页
- *多种角色中的管理员*，第 200 页

委派管理员可管理分配给特定角色的客户端。给每位管理员分配策略权限或报告权限，或者同时分配这两种权限。

具有**策略**权限的委派管理员可将策略应用于分配给其角色的客户端，以确定每个客户端可用的 Internet 访问。作为此职责的一部分，委派管理员可创建、编辑和删除策略和筛选器，但需遵从超级管理员制订的“筛选器锁定”限制。请参阅*定义所有角色的筛选器限制*，第 221 页。

注意

委派的管理员可充分控制所管理的客户端上的 Internet 活动。为确保能此控制能可靠地处理并能遵循您的组织适用的使用策略，超级管理员应使用“审核日志”页监视管理员所作的更改。请参阅*查看并导出审核日志*，第 236 页。

委派管理员不能删除默认策略。

委派管理员可编辑筛选器组件，但有一些限制。请参阅*创建策略和筛选器*，第 206 页，以了解更多信息。

具有策略权限的管理员使用 Websense 用户帐户登录 Websense Manager 时还可更改他们自己的 Websense 密码。（请参阅 *Websense 用户帐户*，第 209 页。）

具有**报告**权限的委派管理员可用的选项取决于配置角色的方式。他们也许只能报告其角色所管理的客户端的情况，也可能可以报告所有客户端的情况。他们可能可以访问所有的报告功能，也可能只能访问有限的报告功能。请参阅*编辑角色*，第 213 页，以了解更多信息。

只有报告权限的管理员仅能使用右侧快捷窗格（“常见任务”和“工具箱”）中有限的选项。

多种角色中的管理员

相关主题：

- *管理员概述*，第 198 页
- *超级管理员*，第 198 页
- *委派管理员*，第 200 页

根据您的组织的需要，同一管理员可以被分配至多个角色。被分配至多个角色的管理员登录时必须选择单一的角色来进行管理。

登录后，您的权限如下：

- **策略**：您可针对登录时选定的角色添加、编辑筛选器和策略，然后将策略应用于该角色所管理的客户端。“委派管理”页列出了您被分配到的所有角色，以便您查看每个角色所管理的客户端和报告权限。
- **报告**：您拥有您所有角色的综合报告权限。例如，假设您分配到 3 个角色，其各自的报告权限如下：
  - 角色 1：无报告
  - 角色 2：仅报告受管理客户端的情况；仅调查报告
  - 角色 3：报告所有客户端的情况；可完全访问所有报告功能

  在这种情况下，无论您在登录时选择哪一种角色，您都可以查看“今天”和“历史”页上的报告，并使用所有的报告功能报告所有客户端的情况。

  如果您登录的角色仅限报告，则横幅窗格中的“角色”字段将表示您拥有的是“全部报告”（报告所有客户端的情况）权限还是“受限报告”（仅报告受管理客户端的情况）权限。

从管理角色开始

相关主题：

- *管理角色概述*，第 197 页
- *通知管理员*，第 203 页
- *委派管理员的任务*，第 204 页

开始使用委派管理则需要超级管理员完成以下任务：

- 确定管理员登录 Websense Manager 的方式。请参阅*启用 Websense Manager 访问*，第 208 页。
- 添加角色并对其进行配置。请参阅*使用委派管理*，第 211 页。
- 通知管理员他们的职责和选项。请参阅*通知管理员*，第 203 页。

除了这些必需的任务之外，还有一些与委派管理相关的可选任务。

创建“筛选器锁定”

无限制超级管理员可创建“筛选器锁定”，以针对所有委派管理角色中的受管理客户端指定要阻止的具体类别和协议。这些限制将针对委派管理角色中创建的所有筛选器或复制到委派管理角色中的所有筛选器自动执行，但委派管理员不能修改这些限制。

> **注意**
>
> “筛选器锁定”不会应用于超级管理员角色管理的客户端。

“筛选器锁定”也可阻止和锁定与选定类别相关的文件类型和关键字，同时强制记录选定的协议。请参阅*创建“筛选器锁定”*，第 221 页。

移动客户端

以超级管理员的身份登录时，在“客户端”页面添加客户端可将此客户端分配给超级管理员角色。“编辑角色”页面不能将将该客户端添加到委派管理角色。理想状态下，您应将此客户端直接添加到角色，而不用在“超级管理员”角色中分配策略。但是，这样做并非总是可行。

要将“超级管理员”角色中的客户端移动到另一个角色，请使用“客户端”页面中的**移动到角色**选项。请参阅*移动客户端到角色*，第 61 页。

作为移动操作的一部分，“超级管理员”角色中应用的策略将复制到委派管理角色。还会复制由策略强制执行的筛选器。在复制过程中，筛选器将进行更新，以执行“筛选器锁定”限制（如果有）。

在目标角色中，选项卡（“已复制”）将添加到筛选器或策略名称的结尾。该角色的管理员可迅速地识别新项目并进行相应更新。

> **注意**
>
> 每次将筛选器或策略复制到同一个角色时，选项卡（“已复制”）将收到随着每次新的复制而递增的数字：（已复制 1）、（已复制 2），依此类推。每一个都将成为角色中单独的筛选器或策略。
>
> 建议角色中的管理员重命名筛选器和策略，并根据需要加以编辑，以明确设置，消除重复项。这些更改可简化日后的维护工作。

超级管理员角色中的全部允许筛选器允许访问全部类别或协议，但不能进行编辑。要保留超级管理员执行“筛选器锁定”的能力，则不能将这些筛选器复制到委派管理角色。

如果被分配给正在移动的客户端的策略执行“全部允许”筛选器，则在您应用未使用“全部允许”筛选器的策略之前，客户端不能移动。

在客户端移动到新角色之后，只有该角色中的管理员才能修改该客户端的策略或其执行的筛选器。“超级管理员”角色中初始策略或筛选器的更改将不会影响委派管理角色中的策略或筛选器副本。

复制筛选器和策略

最初，超级管理员创建的筛选器和策略仅供“超级管理员”角色中的管理员访问。您可使用**复制到角色**选项将筛选器和策略复制到委派管理角色，而不用将客户端移动到此角色。请参阅*将筛选器和策略复制到角色*，第 145 页。

直接复制筛选器和策略时，执行的限制与作为移动客户端的一部分操作而复制筛选器、策略时所应用的限制相同。

- 复制时将执行 “筛选器锁定”限制。
- 不能复制 “全部允许 “类别和协议筛选器。
- 已复制的筛选器和策略采用名称中的选项卡 （“已复制”）在角色中作为标识。

开始复制前应考虑编辑策略描述，以确保它们对目标角色中的管理员有解释意义。

将策略应用于剩余的客户端

未明确分配给委派管理角色的客户端由超级管理员管理。“超级管理员”角色没有 “受管理客户端”列表。

要将策略应用到这些客户端，请将它们添加到“策略管理”>“客户端”页面。请参阅*添加客户端*，第 59 页。尚未分配特定策略的客户端需服从其角色的默认策略。

有时，您可能无法将客户端添加到 “客户端”页。当客户端是分配给其他角色的网络、组、域或组织单位的成员时，就可能会发生这种情况。如果其他角色的管理员已将策略应用到网络或组的单个成员，这些客户端将无法添加到 “超级管理员”角色。

通知管理员

相关主题：

- *管理角色概述*，第 197 页
- *从管理角色开始*，第 201 页

将个人指派为任何管理角色中的管理员后，请确保为他们提供以下信息。

- 登录 Websense Manager 的 URL。默认情况下：

  ```
  https://<ServerIP>:9443/mng/
  ```

  请使用运行 Websense Manager 的计算机的 IP 地址来代替 <ServerIP>。
- 登录时选择哪一个 Policy Server（如适用）。环境中如有多个 Policy Server，管理员必须在登录时选择一个 Policy Server。他们必须选择已配置的 Policy Serve，以与验证其受管理客户端的目录服务进行通讯。
- 登录 Websense Manager 时是使用网络登录帐户还是使用 Websense 用户帐户。如果管理员使用 Websense 用户帐户登录，则应提供用户名和密码。
- 他们的权限是创建策略并将策略应用于角色中的客户端，或者是生成报告，或者是两者兼而有之。

建议具有策略权限和报告权限的管理员考虑计划在会话中执行何种活动。如果他们只计划生成报告，则建议他们转至横幅窗格中的**角色**字段，然后选择**释放策略权限**。这将释放角色的策略权限，使其他管理员能够访问 Websense Manager 并管理该角色的策略。

- 如何找到其角色管理的客户端列表。管理员可转到“策略管理”>“委派管理”，然后单击其角色名称，以显示“编辑角色”页面，该页面包含受管理客户端列表。
- “筛选器锁定”限制 （如有任何类别或协议已被阻止和锁定）。
- 管理员执行的常见任务。请参阅*委派管理员的任务*，第 204 页。

添加或更改自定义文件类型和协议时，请确保通知委派管理员。这些组件将自动出现在所有角色的筛选器和策略中，因此管理员必须知道更改的时间。

委派管理员的任务

相关主题：
- *管理角色概述*，第 197 页
- *从管理角色开始*，第 201 页
- *通知管理员*，第 203 页

具有策略权限的**管理员**可以执行以下任务。

- *查看用户帐户*，第 204 页
- *查看您的角色定义*，第 205 页
- *将客户端添加到“客户端”页面*，第 205 页
- *创建策略和筛选器*，第 206 页
- *将策略应用到客户端*，第 207 页

报告权限可根据细化等级授予。您的角色被授予的特定报告权限将决定具有报告权限的管理员可执行以下哪些任务。请参阅*生成报告*，第 207 页。

查看用户帐户

相关主题：
- *委派管理员的任务*，第 204 页
- *查看您的角色定义*，第 205 页
- *将客户端添加到“客户端”页面*，第 205 页
- *创建策略和筛选器*，第 206 页
- *将策略应用到客户端*，第 207 页

如使用网络凭据登录 Websense Manager，则更改密码需要通过网络目录服务来完成。请与系统管理员联系以获得帮助。

如果您已获得 Websense 用户名和密码，请查看帐户相关信息并在 Websense Manager 中更改密码。

1. 请转到**策略管理 > 委派管理**。
2. 单击页面顶部的**管理 Websense 用户帐户**。
3. 如要更改密码，请单击**更改密码**。请参阅*更改 Websense 用户的密码*，第 211 页。
4. 单击**查看**以显示您以管理员身份参与的角色列表。

查看您的角色定义

相关主题：

- *委派管理员的任务*，第 204 页
- *查看用户帐户*，第 204 页
- *将客户端添加到 “客户端” 页面*，第 205 页
- *创建策略和筛选器*，第 206 页
- *将策略应用到客户端*，第 207 页

打开 “委派管理” 页面，单击您的角色以显示 “编辑角色” 页面，此页面列出了该角色管理的客户端。此页面还将显示角色中具有报告权限的管理员可用的报告功能。

仅具有报告权限的管理员不能查看此页面。这类管理员只能使用指定的报告功能。

将客户端添加到 “客户端” 页面

相关主题：

- *委派管理员的任务*，第 204 页
- *查看用户帐户*，第 204 页
- *查看您的角色定义*，第 205 页
- *创建策略和筛选器*，第 206 页
- *将策略应用到客户端*，第 207 页

超级管理员将向角色分配受管理客户端，但委派管理员必须在应用策略之前将它们添加到 “客户端” 页面。请参阅*添加客户端*，第 59 页，以了解相关说明。

将客户端添加到角色的受管理客户端列表中后，该角色的默认策略就会对这些客户端进行筛选。从超级管理员的“客户端”页面移动到角色的客户端需服从超级管理员采用的策略，这些策略会在移动客户端时随之复制到角色。

在您角色的“委派管理”>“编辑角色”页面中所列出的任何客户端均可以被添加到“客户端”页面并向其分配策略。您还可以添加作为组、域、组织单位或网络范围成员的任何单个用户或计算机，或已分配为您角色中受管理客户端的网络范围。

因为用户可能是多个组、域或组织单位的一部分，因此当不同的角色管理成员相同的组、域或组织单位时，从较大的客户端组添加单个项目可能会引起冲突。如果不同角色中的管理员同时访问 Websense Manager，他们可能会将同一个客户端（例如单个的组成员）添加到其“客户端”页面。在这种情况下，该客户端的 Internet 筛选需服从每个角色建立的优先级。请参阅*管理角色冲突*，第 218 页。

创建策略和筛选器

相关主题：

- *委派管理员的任务*，第 204 页
- *查看用户帐户*，第 204 页
- *查看您的角色定义*，第 205 页
- *将客户端添加到“客户端”页面*，第 205 页
- *将策略应用到客户端*，第 207 页

您的角色在创建后将自动继承预安装的默认策略、类别筛选器和协议筛选器，它们将保持当时定义的状态。但也有一些策略和筛选器可能需要超级管理员进行选择才能复制到您的角色。

除了策略和筛选器之外，您还会继承超级管理员创建的任何自定义文件类型和协议。

您可以自由编辑从超级管理员那里继承的策略和筛选器。您所作的更改将仅影响您的角色。超级管理员如对您以前继承的策略和筛选器进行任何更改，都不会影响您的角色。

注意

登录时超级管理员对自定义文件类型和协议所作的更改将自动影响您角色中的筛选器和策略。

当您的超级管理员通知您这类组件有更改时，请查看您的筛选器和策略，以确保它们能正确处理。

您也可根据需要创建相应数量的新筛选器和策略。由委派管理员创建的筛选器和策略仅供登录进入您的角色的管理员使用。如需创建策略的说明，请参阅*使用策略*，第 64 页。如需创建筛选器的说明，请参阅*筛选器使用*，第 42 页。

您可针对自己的角色编辑筛选器组件，但有一些限制。

- **类别**：添加自定义类别，编辑主数据库和自定义类别，定义其角色中使用的重新分类 URL 和关键字；更改他们创建的类别中默认情况下会应用的操作和高级筛选选项。（对类别的默认操作所作的更改仅在“筛选器锁定”未锁定该类别时才能执行。）
- **协议**：在他们创建的协议筛选器中，更改默认情况下应用的操作和高级筛选选项。（对协议的默认操作所作的更改仅在“筛选器锁定”未锁定该协议时才能执行。）委派管理员不能添加或删除协议定义。
- **文件类型**：查看分配给每个文件类型的文件扩展名。委派管理员不能添加文件类型，也不能更改分配给某个文件类型的扩展名。
- **未筛选的 URL**：添加 URL，并添加表示仅限其角色中所有受管理客户端访问的站点的正规表达式。

更多信息，请参阅*构建筛选器组件*，第 147 页。

如果超级管理员已执行“筛选器锁定”限制，可能有一些类别或协议会被自动阻止，而且不能在您创建和编辑的筛选器中进行更改。请参阅*定义所有角色的筛选器限制*，第 221 页。

将策略应用到客户端

相关主题：

- *委派管理员的任务*，第 204 页
- *查看用户帐户*，第 204 页
- *查看您的角色定义*，第 205 页
- *将客户端添加到“客户端”页面*，第 205 页
- *创建策略和筛选器*，第 206 页

创建策略后，您可将该策略直接应用到已添加到“客户端”页面中的客户端，只需单击**应用到客户端**按钮即可。请参阅*将策略分配给客户端*，第 68 页。

另外，您也可转到“客户端”页面，添加需受此策略控制的客户端。请参阅*使用客户端*，第 52 页。

生成报告

如果您拥有报告权限，则可使用由超级管理员设置的特定报告选项。要了解您可使用的功能，请转到“委派管理”页面，然后单击角色名称。“编辑角色”页面将显示您的权限可使用的报告功能。请参阅*编辑角色*，第 213 页，以了解更多信息。

启用 Websense Manager 访问

配置委派管理角色时，您需确定管理员可访问的 Websense Manager 功能。为确保登录 Websense Manager 的每个人都能获得正确的功能访问权限，每个人都必须使用用户名和密码登录。可使用的帐户类型有两种：

- **网络帐户**将使用您的网络目录服务中已创建的凭据（请参阅 *目录帐户*，第 208 页）。
- **Websense 用户帐户**使您能够创建在 Websense Manager 中专用的用户名和密码（请参阅 *Websense 用户帐户*，第 209 页）。

目录帐户

相关主题：
- *启用 Websense Manager 访问*，第 208 页
- *Websense 用户帐户*，第 209 页

无限制超级管理员可使用**设置 > 常规 > 登录目录**页面输入所需的目录服务信息，以便管理员使用网络凭据登录 Websense Manager。

注意

此信息仅供 Websense Manager 用户验证身份之用。它不适用于筛选客户端。客户端目录服务信息需在“设置”>“目录服务”页面中配置（请参阅 *目录服务*，第 54 页）。

Websense Manager 用户的网络凭据必须通过单一的目录服务进行身份验证。如果您的网络包括多个目录服务，则您在 Websense Manager 中配置的“登录目录”服务和其他服务之间必须存在可信任关系。

如果不能定义单一的目录服务以便和 Websense Manager 一起使用，请考虑为管理员创建 Websense 用户帐户（请参阅 *Websense 用户帐户*，第 209 页）。

要定义 Websense Manager 用于验证管理员身份的目录服务，首先请确保已选定使用目录服务以验证管理员身份的复选框，然后从列表中选择**目录服务**类型。

如选择默认项 **Windows NT Directory / Active Directory (Mixed Mode)**，则无需任何其他设置。单击**确定**以缓存您的更改。直到您单击**全部保存**之后，更改才会生效实施。

如选择 **Active Directory (Native Mode)** 或**其他 LDAP Directory**，请提供以下额外信息：

1. 请输入安装目录服务的计算机的 IP 地址或名称。

   如使用的是 Active Directory (Native Mode)，而且已针对故障转移配置了全局编录服务器，则您可输入 DNS 域名代替。

2. 输入目录服务通讯使用的**端口**。
3. 要使用目录服务加密通讯，请勾选**使用 SSL**。
4. 输入 Websense 软件连接目录服务时需使用的**用户可分辨名称**和**密码**。
5. 输入 Websense 软件验证管理员身份时所使用的**默认域上下文**。
   - 如果您使用的是 Active Directory (Native Mode)，则配置已完成。单击**确定**以缓存您的更改。直到您单击**全部保存**之后，更改才会生效实施。
   - 如您使用的是基于 LDAP 的其他目录服务，请继续。
6. 提供 Websense 软件用来加快用户身份验证速度的**用户登录 ID 属性**和**用户搜索筛选器**（如有）。

   此信息也会显示在**设置 > 目录服务**页面上，即**高级目录设置**下面。如有必要，您可复制和粘贴这些值。
7. 在“组选项”下，指定您的 LDAP 架构是否包括 **memberOf** 属性：
   - 如未使用 memberOf，请指定 Websense 软件用来验证管理员身份的**用户组搜索筛选器**。
   - 如使用了 memberOf，请指定需应用的**组属性**。
8. 如果您的 LDAP 架构包括嵌套组，请勾选**执行其他嵌套组搜索**。
9. 如果您的目录服务使用 LDAP 参考，请指明 Websense 软件应使用还是忽略此参考。
10. 单击**确定**以缓存您的更改。直到您单击**全部保存**之后，更改才会生效实施。

Websense 用户帐户

相关主题：

- *启用 Websense Manager 访问*，第 208 页
- *添加 Websense 用户帐户*，第 210 页

超级管理员使用**委派管理 > 管理 Websense 用户帐户**页面，可为管理员创建不需输入网络目录凭据即可访问的 Websense Manager 帐户。在这一页面，超级管理员也可更改 Websense 用户帐户的密码，查看 Websense 用户被分配为管理员身份的角色。

无限制超级管理员也可从此页面中删除 Websense 用户帐户。

委派管理员可使用此页面更改其 Websense 密码，查看他们被分配为管理员的角色。

选项	描述
添加	打开此页面，以创建新的 Websense 用户帐户。请参阅 *添加 Websense 用户帐户*，第 210 页。
更改密码	打开此页面，以更改相关帐户的密码。请参阅 *更改 Websense 用户的密码*，第 211 页。
查看	显示此用户被分配为管理员的角色列表。
删除	勾选一个或多个废旧用户帐户的复选框，然后单击此按钮将其删除。
关闭	返回 “委派管理”页面。

添加 Websense 用户帐户

相关主题：

- *启用 Websense Manager 访问*，第 208 页
- *Websense 用户帐户*，第 209 页
- *更改 Websense 用户的密码*，第 211 页

使用**委派管理 > 管理 Websense 用户帐户 > 添加 Websense 用户**页面可添加 Websense 用户帐户。

1. 输入一个最多含有 50 个字符的唯一的**用户名**。

   名称长度必须介于 1 至 50 个字符之间，且不得包含下列符号：

   ```
   * < > ' { } ~ ! $ % & @ # . " | \ & + = ? / ; : ,
   ```

   用户名可以包括空格或连接线。
2. 输入此用户的**密码**（4-255 个字符）并予以确认。

   建议使用强密码：8 个字节长或者更长，至少包括以下一项：

   - 大写字母
   - 小写字母
   - 数字
   - 特殊字符 （例如连字号、下划线或空格）
3. 完成更改之后，请单击**确定**以缓存更改并返回 “管理 Websense 用户帐户”页面。直到您单击**全部保存**之后，更改才会生效实施。

更改 Websense 用户的密码

相关主题：

- *启用 Websense Manager 访问*，第 208 页
- *Websense 用户帐户*，第 209 页
- *添加 Websense 用户帐户*，第 210 页

通过**委派管理 > 管理 Websense 用户帐户 > 更改密码**页面委派管理员可更改其 Websense 用户帐户的密码。超级管理员可使用此页面更改任何 Websense 用户帐户的密码。

1. 确定页面顶部显示的是正确的**用户名**。
2. 输入此用户的新**密码**（4-255 个字符）并予以确认。

   建议使用强密码：8 个字节长或者更长，至少包括以下一项：

   - 大写字母
   - 小写字母
   - 数字
   - 特殊字符（例如连字号、下划线或空格）
3. 完成更改之后，请单击**确定**以缓存更改并返回“管理 Websense 用户帐户”页面。直到您单击**全部保存**之后，更改才会生效实施。

使用委派管理

相关主题：

- *管理角色概述*，第 197 页
- *管理角色冲突*，第 218 页

策略管理 > 委派管理页面提供的选项取决于查看此页面的是超级管理员还是委派管理员。

超级管理员可查看当前定义的所有角色的列表，并可使用以下选项。

选项	描述
添加	单击以添加新角色。请参阅*添加角色*，第 212 页。
角色	单击以查看或配置此角色。请参阅*编辑角色*，第 213 页。

选项	描述
删除	单击以删除任何在列表中勾选的角色。此选项仅供无限制超级管理员使用。 请参阅*特殊考量*，第 219 页，以了解删除角色后如何管理角色的客户端的信息。
高级	单击以访问 “管理角色优先级”功能。
管理角色优先级	当受不同角色管理的多个组中存在相同的客户端时，请单击以指定使用哪一个角色的策略设置。请参阅*管理角色冲突*，第 218 页。
管理 Websense 用户帐户	单击以添加、编辑和删除仅用于访问 Websense Manager 的帐户的用户名和密码。请参阅 *Websense 用户帐户*，第 209 页。
管理自定义 LDAP 组	单击以添加、编辑和删除自定义 LDAP 组，以便将其分配为委派管理角色中的受管理客户端。请参阅*使用自定义 LDAP 组*，第 58 页。 如果已配置的目录服务为 Windows NT/Active Directory (Mixed Mode)，此选项不可用。

委派管理员只能查看他们被分配为管理员的角色，而且只能访问有限的选项。

选项	描述
角色	单击以查看分配给角色的客户端和已授予的特定报告权限。请参阅*编辑角色*，第 213 页。
管理 Websense 用户帐户	单击以访问更改 Websense Manager 密码和查看已分配角色的选项。请参阅 *Websense 用户帐户*，第 209 页。

添加角色

相关主题：

- *编辑角色*，第 213 页
- *特殊考量*，第 219 页

使用**委派管理 > 添加角色**页面可提供新角色的名称和描述。

1. 输入新角色的**名称**。

   名称长度必须介于 1 至 50 个字符之间，且不得包含下列符号：

   ```
   * < > ' { } ~ ! $ % & @ # . " | \ & + = ? / ; : ,
   ```

   角色名称可以包括空格或连接线。

2. 输入新角色的**描述**。

   描述最多可以包括 255 个字符。适用于角色名称的字符限制也适用于描述，但有 2 项例外：描述可包括句点 (.) 和逗号 (,)。

3. 单击**确定**以显示**编辑角色**页面，并定义此角色的特征。请参阅*编辑角色*，第 213 页。

   下一次您登录 Websense Manager 时，新角色将添加到横幅窗格中的“角色”下拉菜单中。

编辑角色

相关主题：

- *使用委派管理*，第 211 页
- *添加角色*，第 212 页
- *管理角色冲突*，第 218 页

委派管理员可使用**委派管理 > 编辑角色**页面来查看其角色管理的客户端列表和授予的特定报告权限。

超级管理员可使用此页面来选择某个角色的管理员和客户端，并设置管理权限，具体如下所述。只有无限制超级管理员才能从角色中删除管理员和客户端。

1. 根据需要更改角色**名称**和**描述**。

   注意
   “超级管理员”角色的名称不能更改。

2. 添加和删除此角色的管理员。（此部分仅供超级管理员使用，如果您以委派管理员身份登录，则不会显示此部分。）

项目	描述
用户名	管理员用户名
帐户类型	指明用户是在网络目录服务 （目录）中定义的或者还是被定义为 Websense 用户帐户 (Websense)。
报告	勾选此复选框，以授予使用报告工具的管理员权限。
策略	勾选此复选框，以授予管理员创建筛选器和策略的权限，并将这些策略应用于角色的受管理客户端。 在“超级管理员”角色中，具有策略权限的管理员也可管理某些 Websense 配置设置。请参阅*超级管理员*，第 198 页。

项目	描述
无限制	仅供“超级管理员”角色使用，请勾选此复选框，以授予管理员管理所有 Websense 配置设置和“筛选器锁定”的权限。 只有无限制超级管理员才能向新管理员授予无限制权限。
添加	打开**添加管理员**页面。请参阅*添加管理员*，第 216 页。
删除	从角色中删除在“管理员”列表中勾选的任何管理员。（仅限无限制超级管理员。）

3. 添加和删除该角色的**受管理客户端**。（只有超级管理员才能进行更改。委派管理员可查看分配给其角色的客户端。）

项目	描述
< 名称 >	显示明确分配给其角色的每个客户端的名称。角色中的管理员在应用策略之前必须将客户端添加到“客户端”页面。请参阅*委派管理员的任务*，第 204 页。
添加	打开**添加受管理客户端**页面。请参阅*添加受管理客户端*，第 217 页。
删除	此按钮仅限无限制超级管理员使用，它可从角色中删除受管理客户端列表中勾选的任何客户端。 某些客户端无法从受管理客户端列表中直接删除。请参阅*特殊考量*，第 219 页，以了解更多信息。

4. 使用**报告权限**部分可选择此角色中具有报告访问权限的管理员能够使用的功能。
   a. 选择报告权限的一般级别：

选项	描述
报告所有客户端	选择此选项授予管理员生成有关所有网络用户情况的报告的权限。 使用“报告权限”部分中剩余的选项可设置此角色中管理员的具体权限。
仅报告受管理客户端	选择此选项可限制管理员仅报告分配给此角色的受管理客户端的情况。然后，选择这些管理员可访问的调查报告功能。 受限制仅能报告受管理客户端情况的管理员不能访问“今天”和“历史”页面上的演示报告或基于用户的报告。他们也不能管理日志数据库设置。

b. 找出角色中相应管理员可使用的每种报告功能并勾选这些功能的复选框。

选项	描述
访问演示报告	启用访问演示报告功能。此选项仅在管理员可报告所有客户端的情况时可用。请参阅*演示报告*，第 84 页。
查看 “今天”和 “历史”页上的报告	启用显示图表，以显示这些页面上的 Internet 活动。请参阅*今天：从子夜以来的运行状况、安全和数值情况*，第 20 页和*历史：最近 30 天*，第 23 页。 如果取消选择此选项，管理员只能查看 “今天”页面上的 “运行状况警报”和 “数值情况”部分以及 “历史”页面上的 “估计值”。
访问调查报告	启用访问基本调查报告功能。选择此选项时，也可选择其他的调查报告功能。请参阅*调查报告*，第 100 页。
在调查报告中查看用户名	让此角色中的管理员在登录时可查看用户名。请参阅*配置 Filtering Service 以进行日志记录*，第 257 页。 取消选择此选项，则将仅显示系统生成的身份验证代码，而不显示名称。 此选项仅在管理员获得访问调查报告的权限时才可用。
将调查报告另存为收藏报告	使此角色中的管理员能将调查报告另存为收藏报告。请参阅*收藏调查报告*，第 114 页。 此选项仅在管理员获得访问调查报告的权限时才可用。
计划调查报告	使此角色中的管理员能够安排在日后运行调查报告或反复运行调查报告。 请参阅*计划调查报告*，第 117 页。 此选项仅在管理员获得将调查报告另存在收藏报告的权限时才可用。
管理日志数据库	使管理员能访问 “设置” > “日志数据库”页面。请参阅*日志数据库管理设置*，第 272 页。 此选项仅在管理员可报告所有客户端的情况时可用。

5. 完成更改之后，请单击**确定**以缓存更改并返回 “委派管理”页面。直到您单击**全部保存**之后，更改才会生效实施。

添加管理员

相关主题：

- *编辑角色*，第 213 页
- *启用 Websense Manager 访问*，第 208 页

超级管理员可使用**委派管理 > 编辑角色 > 添加管理员**页面来指定哪些个人在角色中具有管理员身份。

注意

管理员可被添加到多个角色。但在在登录时这些管理员必须选择一个角色。在这种情况下，管理员将获得针对所有角色的综合报告权限。

委派的管理员可充分控制所管理的客户端上的 Internet 活动。为确保能此控制能可靠地处理并能遵循您的组织适用的使用策略，超级管理员应使用“审核日志”页监视管理员所作的更改。请参阅*查看并导出审核日志*，第 236 页。

1. 如果您计划将目录帐号添加为委派管理员，请确保您已登录其“目录服务“配置（请参阅*目录服务*，第 54 页）与“登录目录”配置（请参阅*目录帐户*，第 208 页）相匹配的 Policy Server。

   如果您只是将 Websense 用户帐户添加为管理员，您可登录到任何 Policy Server。

2. 在**目录帐户**下，勾选一个或多个用户的复选框，然后单击右箭头 (>) 按钮将它们移动到**选定**列表。

   注意

   自定义 LDAP 组不能被添加为管理员。

   如果您的环境使用 Active Directory (Native Mode) 或其他基于 LDAP 的目录服务，您可搜索目录，以查找特定用户、组、域或组织部门的名称。请参阅*搜索目录服务*，第 60 页。

3. 在 **Websense 用户帐户**下，勾选一个或多个用户的复选框，然后单击右箭头按钮，将突出显示的用户移动到**选定**列表。

4. 设置此角色中的**管理员权限**。

选项	描述
策略	勾选此选项，使此角色中的管理员能将策略应用于他们的受管理客户端。这样还可以授予某些 Websense 配置设置的访问权限。
无限制	勾选此选项，以授予访问全部 Websense 配置设置的权限。 只有在无限制超级管理员将管理员添加到具有策略权限的超级管理员角色时，此选项才可用。
报告	勾选此选项以授予访问报告工具的权限。使用“编辑角色”页面可设置允许的特定报告功能。

5. 完成更改之后，请单击**确定**返回“编辑角色”页面。
6. 单击“编辑角色”页面上的**确定**，以缓存您的更改。直到您单击**全部保存**之后，更改才会生效实施。

添加受管理客户端

相关主题：

- *使用委派管理*，第 211 页
- *编辑角色*，第 213 页

受管理客户端是分配到角色的用户和计算机，它们的策略由该角色的管理员设置。目录客户端（用户、组、域或组织部门）、计算机和网络都可定义为受管理客户端。

超级管理员可使用**委派管理 > 编辑角色 > 添加受管理客户端**页面，以根据需要添加相应数量的客户端。每个客户端仅可被分配给一个角色。

如果您将网络范围分配为一个角色中的受管理客户端，则不能将该范围中的单个 IP 地址分配给任何其他角色。此外，您不能将一个用户、组、域或组织部门明确分配给 2 个不同的角色。但是，您可将一个用户分配给一个角色，然后再将该用户作为成员所从属的组、域或组织部门分配给另一个角色。

注意

如果某个组是一个角色中的受管理客户端，而且该角色的管理员将策略应用于该组中的每一位成员，则之后不能将该组中的单个用户指定给其他角色。

添加受管理客户端时，请考虑要包括的客户端类型。如将 IP 地址添加到角色，该角色的管理员可报告指定计算机上的**全部**活动。如将用户添加到角色，管理员可报告该用户的全部活动，而无论活动发生在哪一台计算机上。

在管理员管理的角色中，管理员不会自动归入受管理客户端，因为这样会使他们能够设置自己的策略。要使管理员能够查看他们自己的 Internet 使用情况，请启用自我报告 （请查阅 *自我报告*，第 284 页）。

如果您的组织已部署多个 Policy Server，而且 Policy Server 与不同的目录通讯，请确保选择与您要添加的客户端所处的目录相连接的 Policy Server。

注意
最佳规程表明，同一个角色中的所有受管理客户端应源于同一个目录服务。

1. 选择角色的客户端：
   - 在**目录**下，勾选一个或多个用户的复选框。
     如果您的环境使用 Active Directory (Native Mode) 或其他基于 LDAP 的目录服务，您可搜索目录，以查找特定用户、组、域或组织部门的名称。请参阅 *搜索目录服务*，第 60 页。
   - 在**计算机**下，输入要添加到此角色的计算机的 IP 地址。
   - 在**网络**下，输入要添加为一个单位的多台计算机的第一个和最后一个 IP 地址。
2. 单击与客户端类型相邻的右箭头 (>) 按钮，将客户端移动到**选择的**列表。
3. 完成更改之后，请单击**确定**返回 “编辑角色” 页面。
4. 单击 “编辑角色” 页面上的**确定**，以缓存您的更改。直到您单击**全部保存**之后，更改才会生效实施。

管理角色冲突

相关主题：
- *使用委派管理*，第 211 页
- *添加受管理客户端*，第 217 页

目录服务允许同一个用户从属于多个组。因此，一个用户可能存在于由不同委派管理角色所管理的多个组中。域和组织机构也存在同样的情况。

此外，用户可能由一个角色管理，也可能属于由不同角色管理的组、域或组织单位。如果这两个角色的管理员同时登录，则当负责组的管理员将策略应用于单个的组成员时，负责用户的管理员可将策略应用于该用户。

使用**委派管理 > 管理角色优先级**页面可设定 Websense 软件在由于重叠不同策略应用于同一个用户时该如何操作。发生冲突时，Websense 软件将应用此列表中显示位置最靠上的角色中的筛选策略。

1. 选择列表中除超级管理员之外的任何角色。

注意
超级管理员角色始终是列表中的第一个。它无法移动。

2. 单击**上移**或**下移**以更改它在列表中的位置。
3. 重复步骤 1 和 2，直到所有角色都具有所需的优先级。
4. 完成更改之后，请单击**确定**以缓存更改并返回“委派管理”页面。直到您单击**全部保存**之后，更改才会生效实施。

特殊考量

相关主题：
- *使用委派管理*，第 211 页
- *编辑角色*，第 213 页

删除委派管理角色或从角色中删除受管理客户端之前，请查看以下信息。

删除角色

在**委派管理**页面，无限制超级管理员可删除任何废旧角色。

删除角色也会删除该角色管理员已添加到“客户端”页面的所有客户端。删除角色后，如这些客户端属于任何由其他角色管理的网络、组或域，它们需服从那些角色中应用的相应策略（请参阅*筛选顺序*，第 68 页）。否则，它们需服从超级管理员的默认策略。

1. 在**委派管理**页面，勾选要删除的每个角色旁的复选框。

   注意
   您不能删除超级管理员角色。

2. 单击**删除**。
3. 确认删除请求，从“委派管理”页面删除选定的角色。只有单击**全部保存**之后，更改才会永久生效。

   下一次您登录 Websense Manager 时，已删除角色将从横幅窗格中的“角色”下拉菜单中清除。

删除受管理客户端

在下列情况下，无法直接从受管理客户端列表（委派管理 > 编辑角色）中删除客户端：

- 管理员已将策略应用于客户端
- 管理员已将一个策略应用于网络、组、域或组织单位的一个或多个成员

如果超级管理员在登录 Websense Manager 时没有选择与包含要删除客户端的目录服务进行通讯的 Policy Server，而选择了其他的 Policy Server，也可能会引发问题。在这种情况下，当前 Policy Server 和目录服务将不会识别客户端。

无限制超级管理员可确保删除相应客户端，具体如下。

1. 登录 Websense Manager，选择其目录服务包含要删除的受管理客户端的 Policy Server。您必须以无限制超级管理员权限登录。
2. 打开横幅窗格中的**角色**列表，然后选择要删除的客户端所属的角色。
3. 转到**策略管理 > 客户端**查看委派管理员已明确分配策略的所有客户端列表。

   这可能包括角色的受管理客户端列表中明确标识的客户端和受管理客户端列表中网络、组、域或组织单位成员的客户端。
4. 删除相应的客户端。
5. 单击**确定**以缓存更改。
6. 打开横幅窗格中的**角色**列表，选择**超级管理员**角色。
7. 转到**策略管理 > 委派管理 > 编辑角色**。
8. 从受管理客户端列表中删除相应的客户端，然后单击**确定**以确认删除请求。
9. 单击“编辑角色”页面上的**确定**以缓存更改。直到您单击**全部保存**之后，更改才会生效实施。

多个管理员访问 Websense Manager

相关主题：

- *管理员概述*，第 198 页
- *启用 Websense Manager 访问*，第 208 页

不同角色中的管理员可同时访问 Websense Manager，以执行其角色权限允许的任何活动。例如，角色 A 和角色 B 中的管理员如果都具有策略权限，他们可同时登录 Websense Manager。由于他们管理不同的客户端，因此当他们创建和应用策略时并不会引起冲突。

如果同一个角色中拥有策略权限的管理员同时登录的话，则情况将有所不同。为确保策略结构和分配的完整性，一次只允许一个角色中一名具有策略权限的管理员访问 Websense Manager。如果该角色中第二个具有策略权限的管理员在第一个管理员仍处于登录状态时尝试登录，则该第二个管理员会获得一个选择。

- 如果此管理员具有报告权限，可登录仅执行报告活动。
- 如果此管理员已分配了任何其他角色，可登录到其他角色。
- 在第一个管理员注销后再试。

同时具有策略权限和报告权限的管理员登录以生成报告时，他们应立即释放其策略权限，以便该角色中的其他管理员可执行策略管理活动。

- 转到横幅窗格中的**角色**下拉菜单，选择**释放策略权限**。

另一种方法是创建每个角色的特殊 Websense 用户帐户 （请参阅 *Websense 用户帐户*，第 209 页）并仅给该用户授予报告权限。将登录凭据 （用户名和密码）提供给角色中具有策略权限和报告权限的管理员。当管理员需要运行报告时，他们可以以该报告管理员的身份登录，以便其他管理员执行策略活动。

定义所有角色的筛选器限制

相关主题：

- *管理员概述*，第 198 页
- *创建 “筛选器锁定”*，第 221 页

Websense 软件允许无限制超级管理员建立 “筛选器锁定”，阻止委派管理角色管理的所有客户端的类别和协议。请参阅 *创建 “筛选器锁定”*，第 221 页，以了解更多信息。

这类角色的管理员可将任何筛选操作应用于其策略中的其他类别和协议，但不允许应用于 “筛选器锁定”中阻止的类别和协议。

针对所有受管理客户端所作的 “筛选器锁定”更改在更改保存后将立即执行。更改生效后，正在使用 Websense Manager 的委派管理员只有在下一次登录时方可查看其筛选器中的更改。

注意

筛选器从超级管理员角色复制到另一个角色时，此复制操作需服从 “筛选器锁定”的限制。

超级管理员不受 “筛选器锁定”的限制。他们可定义允许委派管理角色访问被阻止和被锁定类别和协议的策略。因此，需要特殊访问权限的个人应由超级管理员角色管理。

创建 “筛选器锁定”

相关主题：

- *定义所有角色的筛选器限制*，第 221 页
- *锁定协议*，第 222 页
- *锁定协议*，第 223 页

策略管理 > 筛选器锁定页面中您可以选择是否编辑要阻止委派管理角色中所有受管理客户端访问的类别或协议。任何已在 “筛选器锁定”中阻止的类别或协议功能均被视为**已阻止和锁定**。

- 单击**类别**按钮以阻止和锁定特定的类别或类别元素（关键字和文件类型）。请参阅 *锁定协议*，第 222 页。
- 单击**协议**按钮以阻止和锁定协议或协议的记录。请参阅 *锁定协议*，第 223 页。

锁定协议

相关主题：

- *定义所有角色的筛选器限制*，第 221 页
- *创建 “筛选器锁定”*，第 221 页
- *锁定协议*，第 223 页

使用**策略管理 > 筛选器锁定 > 类别**页面以选择要阻止和锁定委派管理角色中所有成员访问的类别。您还可以阻止和锁定类别的关键字和文件类型。

1. 在树中选择一个类别。

   委派管理角色没有访问超级管理员创建的自定义类别的权限。因此，自定义类别不会出现在树中。
2. 在类别树旁边的框中设置此类别的限制。

选项	描述
锁定类别	阻止和锁定对此类别站点的访问。
锁定关键字	根据每个角色中针对此类别定义的关键字阻止和锁定访问。
锁定文件类型	阻止和锁定针对此类别中站点选定的文件类型。 请确保勾选每个要阻止和锁定的文件类型的复选框。 此列表包括超级管理员创建的自定义文件类型，因为委派管理角色可以使用这些类型。
应用到子类别	将相同的设置应用于此类别的所有子类别。

   您可立即阻止和锁定所有类别的选定元素（如适合）。选择树中的**所有类别**，然后选择所有类别中要阻止的元素。之后，单击**应用到子类别**。
3. 完成更改之后，请单击**确定**以缓存更改并返回 “筛选器锁定” 页面。直到您单击**全部保存**之后，更改才会生效实施。

锁定协议

相关主题：

- *定义所有角色的筛选器限制*，第 221 页
- *创建 “筛选器锁定”*，第 221 页
- *锁定协议*，第 222 页

使用**策略管理 > 筛选器锁定 > 协议**页面，以针对委派管理角色管理的所有客户端阻止和锁定访问所选协议或锁定所选的协议记录。

注意

协议记录与协议使用警报相关。除非在至少一个协议筛选器中设置对协议进行记录，否则您不能生成协议的使用警报。通过 “筛选器锁定”启用**锁定协议记录**选项可确保生成协议使用警报。请参阅*配置协议使用警报*，第 243 页。

1. 在树中选择一个协议。

   委派管理角色可访问超级管理员创建的自定义协议。因此，自定义协议会出现在树中。
2. 在协议树旁边的框中设置此协议的限制。

选项	描述
锁定协议	阻止和锁定访问使用此协议的应用程序和 Web 站点。
锁定协议记录	记录有关访问此协议的信息，并阻止委派管理员禁用记录。
应用到组	将相同设置应用到组中的所有协议。

3. 完成更改之后，请单击**确定**以缓存更改并返回 “筛选器锁定”页面。直到您单击**全部保存**之后，更改才会生效实施。

12 Websense Server 管理

相关主题：

- *Websense 产品组件*，第 226 页
- *与 Policy Server 协同工作*，第 231 页
- *查看并导出审核日志*，第 236 页
- *停止和启动 Websense 服务*，第 238 页
- *警报*，第 239 页
- *备份并还原您的 Websense 数据*，第 246 页

Internet 使用情况筛选需要由多项 Websense 软件组件之间的互动来完成：

- 用户的 Internet 访问请求是由 Network Agent 或第三方集成产品来接收。
- 请求会发送至 Websense Filtering Service 进行处理。
- Filtering Service 与 Policy Server 和 Policy Broker 进行通讯，以对请求作出回应并采用恰当的策略。

在多数情况下，无论设有一个或多个 Policy Database，一个 Policy Database 中会储存客户端、筛选器、策略和一般性配置信息。

Websense Manager 的每个实例都与单一的 Policy Database 相关联，可用于配置与该数据库相关联的每个 Policy Server。

由于 Websense Manager 中所执行的策略配置被储存在中央数据库中，策略信息会自动提供给与该 Policy Database 相关联的全部 Policy Server。

Websense 产品组件

相关主题：

- *筛选组件*，第 227 页
- *Reporting 组件*，第 229 页
- *用户标识组件*，第 229 页
- *与 Policy Server 协同工作*，第 231 页
- *停止和启动 Websense 服务*，第 238 页
- *查看当前系统状态*，第 245 页

Websense 软件由多项协同工作的组件所组成，可提供用户标识、Internet 筛选，以及报告功能。本部分中会提供每个组件的概况，以帮助您理解并管理您的筛选环境。

Websense 的主要组件包括：

- Policy Database
- Policy Broker
- Policy Server
- Filtering Service
- Network Agent
- Master Database
- Websense Manager
- Usage Monitor
- User Service
- Log Server
- Log Database

Websense 软件还包含可选的透明标识代理：

- DC Agent
- RADIUS Agent
- eDirectory Agent
- Logon Agent

其他可选组件包括：

- Remote Filtering Server
- Remote Filtering Client
- Websense Content Gateway

筛选组件

组件	描述
Policy Database	存储 Websense 软件设置和策略信息。
Policy Broker	管理来自 Websense 组件的策略与一般性配置信息请求。
Policy Server	• 识别并追踪其他 Websense 组件的位置和状态。 • 储存特定单个 Policy Server 实例的配置信息。 • 通讯至 Filtering Service 的配置数据，以供筛选 Internet 请求使用。 配置 Websense Manager 中的 Policy Server 设置（请参阅 *与 Policy Server 协同工作*，第 231 页）。 拥有相同 Policy Database 的 Policy Server 之间可共享策略和大多数配置设置（请参阅 *在多个 Policy Server 环境下工作*，第 232 页）。
Filtering Service	与 Network Agent 或第三方集成产品配合提供 Internet 筛选。当用户提出站点请求时，Filtering Service 会收到请求并决定采用哪种策略。 • 必须运行 Filtering Service 以对 Internet 请求进行筛选和记录。 • 每个 Filtering Service 实例均会下载各自的 Websense 主数据库副本。 Websense Manager 中配置的筛选和 Filtering Service 操作（请参阅 *Internet 使用情况筛选器*，第 33 页和 *配置 Websense 筛选设置*，第 49 页）。
Network Agent	• 改进筛选和记录功能 • 启用协议管理 • 启用独立环境下的筛选 更多信息，请参阅 *网络配置*，第 287 页。
Master Database	• 包含按 90 多个类别和子类别加以分类的超过 3600 万个网站 • 包含超过 100 项可供筛选协议使用的协议定义 下载 Websense 主数据库可激活 Internet 筛选，并确保数据库会不断更新。如果主数据库超过 2 周时间，则不会进行筛选。请参阅 *Websense 主数据库*，第 28 页，以了解更多信息。
Websense Manager	作为 Websense 软件的配置和管理接口。 使用 Websense Manager 可定义和自定义 Internet 访问策略、添加或删除筛选客户端、配置 Websense 软件组件等。 请参阅 *使用 Websense Manager*，第 16 页，以了解更多信息。

组件	描述
Usage Monitor	根据 Internet 使用情况启用警报。 Usage Monitor 会追踪 URL 类别和协议访问，并根据您所配置的警报操作生成警报消息。 请参阅 *警报*，第 239 页，以了解更多信息。
Remote Filtering Client	• 位于网络防火墙外部的客户端计算机上。 • 识别要筛选的客户端计算机，并与 Remote Filtering Server 通讯。 请参阅 *Filter Remote 客户端*，第 133 页，以了解更多信息。
Remote Filtering Server	• 允许网络防火墙外部客户端筛选。 • 与 Filtering Service 通讯，提供远程计算机的 Internet 访问管理。 请参阅 *Filter Remote 客户端*，第 133 页，以了解更多信息。
Websense Content Gateway	• 提供坚实的代理和缓冲平台。 • 可以实时分析网站和文件的内容，将以前尚未分类的站点加以分类。 请参阅 *分析带实时选项的内容*，第 123 页。
Websense Security Gateway	除了 Websense Content Gateway 的标准功能之外，还能够： • 分析 HTML 代码以查找安全威胁 （例如网络钓鱼、URL 跳转、网络漏洞攻击病毒，以及代理规避）。 • 检查文件内容并为其分配威胁类别（例如病毒、木马、或蠕虫）。 • 从特定网页中剥离有效内容。 请参阅 *分析带实时选项的内容*，第 123 页。

Reporting 组件

组件	描述
Log Server	记录 Internet 请求数据，包括： • 请求来源 • 与请求相关的类别或协议 • 请求已被允许或是阻止 • 是否采用了键盘阻止、文件类型组织、定额分配、带宽级别或密码保护 利用 Network Agent 和某些集成产品，Log Server 还会储存关于带宽用量的信息。 Log Server 必须安装在 Windows 计算机上才能启用 Websense Manager 之中的调查报告或演示报告，以及“今天”和“历史”页面图表。 安装 Log Server 之后，配置 Filtering Service 以使记录数据被传送至正确的位置（请参阅*配置 Filtering Service 以进行日志记录*，第 257 页）。
Log Database	储存由 Log Server Stores 所收集以供 Websense 报告工具所使用的 Internet 请求数据。

用户标识组件

组件	描述
User Service	• 与您的目录服务通讯。 • 传送至 Policy Server 和 Filtering Service 中的用户相关信息，包括在采用的筛选策略中所使用的用户与组及用户与域的关系。 如果您已安装并配置了 Websense 透明标识代理（请参阅*透明标识*，第 169 页），User Service 会帮助解析用户登录会话信息，并使用此信息向 Filtering Service 提供用户名与 IP 地址的关联。 当您将用户和组添加为 Websense 客户端后（请参阅*添加客户端*，第 59 页），User Service 会从 Websense Manager 的目录服务中提供名称和路径信息。 有关配置目录服务访问的信息，请参阅*目录服务*，第 54 页。
DC Agent	• 为使用基于 Windows 目录服务的用户提供透明用户标识。 • 与 User Service 通讯，为 Websense 软件提供最新的用户登录会话信息以供筛选之用。 更多信息，请参阅 *DC Agent*，第 178 页。

组件	描述
Logon Agent	• 在 Linux 和 Windows 网络中提供最准确的透明用户标识。 • 在捕获用户登录会话时不依赖于目录服务或其他中介程序。 • 在用户登录会话开始时即探测到其出现。 Logon Agent 与客户端计算机上的登录应用程序进行通讯，确保个人用户的登录会话被 Websense 软件捕获并直接处理。 更多信息，请参阅 *Logon Agent*，第 181 页。
eDirectory Agent	• 与 Novell eDirectory 协作，透明地识别用户。 • 从验证用户网络登录的 Novell eDirectory 中收集用户的登录会话信息。 • 将每个验证用户与 IP 地址相关联，然后与 User Service 协作向 Filtering Service 提供信息。 更多信息，请参阅 *eDirectory Agent*，第 187 页。
RADIUS Agent	支持对通过拨号上网、虚拟专用网络 (VPN)、数字用户线 (DSL)、或其他远程连接来访问网络的用户进行透明标识。 更多信息，请参阅 *RADIUS Agent*，第 183 页。

了解 Policy Database

Websense Policy Database 可同时储存策略数据 （包括客户端、筛选器、筛选器组件，以及委派的管理设置）和为 Websense Manager 指定的全局配置设置。专门为单个 Policy Server 实例所指定的设置将单独储存。

在大多数的多个 Policy Server 环境下，单个 Policy Database 可存储多个 Policy Server 的策略和一般性配置数据。

1. 在启动时，每个 Websense 组件会通过 Policy Broker 向 Policy Database 请求适用的配置信息。
2. 运行组件时常常会检查对于 Policy Database 的更改。
3. 当管理员每次在 Websense Manager 中进行更改并单击 “全部保存” 之后，Policy Database 均会更新。
4. 当 Policy Database 进行更改之后，每个组件都会请求并收到影响其功能的更改内容。

定期对 Policy Database 进行备份，以确保重要配置和策略信息的安全。请参阅*备份并还原您的 Websense 数据*，第 246 页，以了解更多信息。

与 Policy Server 协同工作

Policy Server 是 Websense 软件中用于管理策略信息并与 Filtering Service 通讯以在策略执行中提供帮助的组件。Policy Server 还负责识别其他组件并追踪其位置和状态。

当您登录 Websense Manager 之后，还将登录 Policy Server 的图形界面。

- 在配置 Websense Manager 可与 Policy Server 进行通讯之前，您不能登录 Websense Manager。
- 如果您的 Websense 软件安装中包含多个 Policy Server，登录时您可以在各个 Policy Server 实例中进行选择。
- 您可以在 Websense Manager 中添加和删除 Policy Server 实例。

默认情况下， Websense Manager 与中央 Policy Server 实例之间的通讯将在 Websense Manager 安装时建立。

多数情况下只要求一个 Policy Server 即可。单个 Policy Server 可与多项 Filtering Service 和 Network Agent 实例通讯以实现负载均衡。但是，在非常庞大的机构（超过 10,000 名用户）内，安装多个 Policy Server 实例可能会有所帮助。如果您安装了额外的 Policy Server，请将每个实例添加至 Websense Manager 中 （请参阅*添加并编辑 Policy Server 实例*，第 232 页）。

添加并编辑 Policy Server 实例

利用**设置 > Policy Server** 页面将 Policy Server 实例添加至 Websense Manager 中，或是配置或删除现有的 Policy Servers。

要添加 Policy Server 实例：

1. 单击**添加**。“添加 Policy Server”页面会打开。
2. 在**服务器名称或 IP** 字段中输入 Policy Server 计算机的 IP 地址或主机名称。
3. 输入 Websense Manager 用于与 Policy Server 实例通讯的**端口**。默认值为 **55806**。
4. 单击**确定**返回 Policy Server 页面。新的 Policy Server 实例会出现在列表之中。
5. 单击**确定**，将所有更改缓存至 Policy Server 页面。直到您单击**全部保存**之后，更改才会生效实施。

要编辑 Policy Server 实例（例如，如果 Policy Server 计算机的 IP 地址或名称变更），选择 Policy Server 列表中的一个 IP 地址或主机名称，然后单击**编辑**。

要删除 Policy Server 实例，请选择 Policy Server 列表中的一个 IP 地址或主机名称，然后单击**删除**。单击“删除”会将 Policy Server 实例从 Websense Manager 中删除，但是不会卸载或停止 Websense Policy Server 服务。如果仅列有一个 Policy Server 实例，您无法将其删除。

在多个 Policy Server 环境下工作

在用户数量较大的分布式环境下，安装多个 Policy Server 可能会较为适合。但这可能会导致一些特殊考量。

- 如果您执行了允许不同 Policy Server 来管理同一客户端的配置，根据当前的负载情况，**不要**执行基于时间的策略操作：
  - 密码替代
  - 确认
  - 定额

  与此功能相关的定时信息不会在 Policy Server 之间共享，而客户可能会获得比您计划的更多或更少的 Internet 访问。

  请记住，当对客户端没有采用其他任何策略时，即会执行默认策略。如果客户端可以接受多个 Policy Server 的管理，您需要确保不会在采用了基于时间操作的类别筛选器中执行默认策略。
- 由于策略信息储存于 Policy Database 之中，当您单击**全部保存**后，策略更改将自动由所有 Policy Server 共享。
- 许多全局配置设置（如风险级别定义和警报选项）也会在 Policy Server 之间共享。
- 针对单个 Policy Server 的配置设置（如 Filtering Service 和 Network Agent 连接）会储存在每个 Policy Server 的本机位置上，而不会分布散播。

要在 Websense Manager 的 Policy Server 之间切换以查看或配置应用于单个 Policy Server 实例的设置：

1. 在 Websense 横幅窗格中，展开 **Policy Server** 列表并选择一个 IP 地址。
2. 如果当前 Policy Server 实例中有未保存的更改，则会显示更改列表。执行下列操作之一：
   - 单击**全部保存和退出**，保存更改并退出当前的 Policy Server。
   - 单击**取消更改和退出**，放弃更改并退出当前的 Policy Server。
   - 单击**返回**，继续配置当前 Policy Server。

   如果没有未保存的更改，您将直接转至登录屏幕。
3. 在登录屏幕中输入用户名和密码以登录选中的 Policy Server，然后单击**登录**。

更改 Policy Server 的 IP 地址

在更改 Policy Server 计算机的 IP 地址之前，**停止计算机上的所有 Websense 服务**。如果该计算机上还安装了 Websense Manager，这其中还包括 Apache2Websense 和 ApacheTomcatWebsense 服务。

当更改 IP 地址之后，在恢复筛选之前，您必须手动更新 Websense Manager、Policy Server，以及其他 Websense 服务所使用的 Websense 配置文件。

步骤 1：更新 Websense Manager 配置

更新 Websense Manager，以使用新的 IP 地址来连接 Policy Server。

1. 在 Websense Manager 计算机上，停止 **Apache2Websense** 和 **ApacheTomcatWebsense** 服务 （如必要）。

   如果此计算机上同时安装了 Websense Manager 和 Policy Server，Apache 服务应已被停止。
2. 转至下列目录：
   - Windows：

     `C:\Program Files\Websense\tomcat\conf\Catalina\localhost\`
   - Linux：

     `/opt/Websense/tomcat/conf/Catalina/localhost/`
3. 找到 **mng.xml** 文件，将其备份至另一个目录。
4. 用文本编辑器（如记事本或 vi）打开 **mng.xml** 并将每个实例的旧 IP 地址替换为新 IP 地址。

   Policy Server 的 IP 地址会出现两次：作为 **ps/default/host** 的值和 **psHosts** 的值。
5. 完成后，保存并关闭文件。

在完成本部分余下的配置更新之前，不要重新启动 Apache 服务。

步骤 2：更新 Policy Server 配置

更新 Policy Server 配置文件，以及用于配置 Websense 各组件之间通讯的初始化文件。

1. 如果您还未这样操作，请停止 Policy Server 计算机上的所有 Websense 服务（请参阅*停止和启动 Websense 服务*，第 238 页）。
2. 转至 Websense 的 **bin** 目录。
   - Windows：

     ```
     C:\Program Files\Websense\bin
     ```

   - Linux

     ```
     /opt/Websense/bin
     ```

3. 找到 **config.xml** 文件，将其备份至另一个目录。
4. 用文本编辑器打开 **config.xml** 并将每个实例的旧 IP 地址替换为新 IP 地址。
5. 完成后，保存并关闭文件。
6. 在 **bin** 目录中找到 **websense.ini** 文件，将其备份至另一个目录。
7. 用文本编辑器打开 **websense.ini** 并将每个实例的旧 IP 地址替换为新 IP 地址。
8. 完成后，保存并关闭文件。

步骤 3：验证日志数据库连接

在 Policy Server 计算机上使用 Windows ODBC Data Source Administrator，验证 ODBC 与日志数据库的连接。

1. 前往**开始 > 设置 > 控制面板 > 管理工具 > 数据源 (ODBC)**。
2. 在**系统 DSN** 选项卡中选择合适的数据源名称（默认为 **wslogdb70**），然后单击**配置**。
3. 验证已选择了正确的数据库服务器计算机，然后单击**下一步**。
4. 输入用于连接数据库的凭据，然后单击**下一步**。
5. 在下面两个屏幕中接受默认设置，然后单击**测试数据源**。

> **注意**
>
> 如果测试失败，检查数据库服务器计算机的名称并重试。
>
> 如果计算机名称正确但是测试仍然失败，检查是否使用了正确的连接端口，以及防火墙对于所选端口是否允许通讯。

步骤 4：重新启动 Websense 服务

1. 重新启动 Policy Server 计算机。确保该计算机上的所有 Websense 服务都正常地重新启动。

2. 如果用于配置此 Policy Server 的 Websense Manager 被安装在另一台计算机上，则重新启动那台计算机上的 **Apache2Websense** 和 **ApacheTomcatWebsense** 服务。

注意

如果 Websense Manager 与 Policy Server 被安装在同一台计算机上，管理员必须使用新的 IP 地址登录。

与 Filtering Service 协同工作

Filtering Service 是 Websense 软件的一个组件，可与 Network Agent 或第三方集成产品协同工作来筛选 Internet 活动。当用户提出一个站点请求时， Filtering Service 会接到请求，决定采用哪种策略，并根据适用的策略来决定如何对该站点进行筛选。

每项 Filtering Service 实例会下载其各自的 Websense 主数据库副本，用以决定如何筛选 Internet 请求。

Filtering Service 还会向 Log Server 发送关于 Internet 活动的信息，使其能够被记录并用于报告。

当您登录 Websense Manager 时，“状态”>“今天”页面中的 **Filtering Service 摘要**将列出与当前 Policy Server 相关的每个 Filtering Service 实例的 IP 地址和当前状态。单击 Filtering Service 的 IP 地址，了解关于所选 Filtering Service 的更多详细信息。

查看 Filtering Service 详细信息

利用**状态 > 今天 > Filtering Service 详细信息**页面查看单个 Filtering Service 实例的状态。

该页面将列出：

- Filtering Service 的 IP 地址
- 所选的实例是否在运行
- Filtering Service 版本

  这应与您的 Websense 软件版本相匹配，包括所采用过的任何修补程序。
- Filtering Service 计算机上运行的操作系统
- Websense 软件平台

  这将指明 Websense 软件是在独立模式下运行还是与第三方产品集成运行。
- 与所选 Filtering Service 通讯的任何 Network Agent 实例的 IP 地址和状态。

单击**关闭**返回 “今天”页面。

查看主数据库的下载状态

您网络中的每个 Filtering Service 实例会下载各自的主数据库副本。当您使用 Websense Manager 时，“状态”>“今天”页面中的运行状况警报摘要会在主数据库下载进行中、或下载尝试失败时显示状态消息。

关于近期或进行中数据库下载的详细信息，请单击 “今天”页面工具栏中的**数据库下载**。数据库下载页面中包含针对每个与当前 Policy Server 相关联之 Filtering Service 实例的条目。

起初，数据库下载页面会显示快速下载摘要，展示下载数据库的哪个部分、哪个版本，以及下载是否成功。从该摘要视图中，您可以：

- 启动针对单个 Filtering Service 数据库下载 （单击**更新**）。
- 为所列出的全部 Filtering Service 实例启用数据库下载 （单击**全部更新**）。
- 取消一项或全部进行中的更新。

单击右侧列表中的一个 IP 地址以查看所选 Filtering Service 的数据库下载状态详细信息。

- 如果所选的 Filtering Service 遇到下载问题，可能会显示对解决该问题的建议。
- 要手动启动所选 Filtering Service 的数据库下载，请单击**更新**。

在数据库下载过程中，状态屏幕会显示下载流程中每个阶段的详细进程信息。单击**关闭**以隐藏进程信息，并继续使用 Websense Manager。

可恢复的主数据库下载

如果 Master Database 下载中断， Websense 软件会自动尝试恢复下载。如果 Filtering Service 能够重新连接下载服务器，则下载会从中断点处恢复。

您可以手动重新开始一项失败或中断的下载。这不能使下载从中断点处恢复，但是可以从起始处重新启动流程。

1. 在 Websense Manager 中，前往**状态 > 今天**并单击**数据库下载**。
2. 单击**停止所有更新**以停止中断的进程。
3. 选择 Filtering Service 实例并单击**更新**，或单击**全部更新**，从起始处重新启动下载流程。

查看并导出审核日志

Websense 软件提供审核追踪，可显示哪位管理员访问了 Websense Manager，以及对策略和设置所做的任何更改。此信息仅供被授予策略权限的超级管理员使用（请参阅*超级管理员*，第 198 页）。

委派的管理员可充分控制所管理的客户端上的 Internet 活动。通过审核日志来监视其更改令您可以确保这项控制得到了负责任的处理，并符合贵机构可接受的使用策略。

使用**状态 > 审核日志**页面可查看审核日志，并可将其中选定的部分导出至 Excel 电子表格 （XLS）文件中 （如需要）。

审核记录将保存 60 天。要想将审核记录保存超过 60 天，请使用导出选项对日志实施定期导出。导出操作不会删除审核日志中的记录。

当导出日志页面打开时，将显示最近的记录。使用日志上方的滚动栏和分页按钮可查看较早的记录。

日志中会显示下列信息。如果某一项被删减，单击该部分项可在弹出式对话框中显示完整记录。

列	描述
日期	更改的日期和时间，会根据时区不同而调整。 要确认审核日志中的数据一致性，请确保运行 Websense 组件的所有计算机上都同步设置了日期和时间。
用户	进行更改的管理员用户名。
服务器	受到更改影响的运行 Policy Server 计算机的 IP 地址或名称。 这只会在影响 Policy Server 的更改中出现，如在“设置”选项卡中进行的更改。
角色	受到更改影响的委派管理角色。 当更改对一个被明确分配为受委派管理员角色管理的客户端产生影响时，该更改会显示为影响超级管理员角色。如果更改对于隶属于一个网络范围、组、域的成员客户端或分配至该角色的组织单位的客户端产生了影响，则更改会显示为影响委派管理员角色。
类型	被更改的配置元素，如策略、类别筛选器或登录 / 退出。
元素	所更改特定对象的标识符，如类别筛选器名称或角色名称。
操作	所做更改的类型，如添加、删除、更改、登录等。
上一个	更改之前的值。
当前	更改之后的新值。

不是所有记录的全部项目均会被显示。例如，登录和退出记录中将不会显示角色。

要导出审核日志记录：

1. 从**导出范围**列表中选择一个时段。

   选择**最近 60 天**可导出整个审核日志文件。

2. 单击**开始**。

   如果在运行 Websense Manager 的计算机上安装有 Microsoft Excel，则会打开导出文件。使用 Excel 中的选项可保存或打印文件。

   如果在运行 Websense Manager 的计算机上未安装 Microsoft Excel，请依照屏幕上的说明来查找软件或保存文件。

停止和启动 Websense 服务

Websense 服务被配置为计算机每次重新启动时都随之启动。但是，在某些情况下您需要在计算机重新启动时单独停止或启动一项或多项产品组件。

> **注意**
> 如果 Filtering Service 正在下载主数据库，则它在下载完毕之前不会停止运行。

当您停止所有 Websense 服务之后，通常会依照所显示的顺序停止下列服务：

1. Websense Policy Server
2. Websense Policy Broker
3. Websense Policy Database

请注意，除非问题与 Policy Broker 或 Policy Database 特定相关，否则通常不需要重新启动这些服务。应尽可能避免重新启动这些服务。

当您启动所有 Websense 服务之后，通常会依照所显示的顺序启动下列服务：

1. Websense Policy Database
2. Websense Policy Broker
3. Websense Policy Server

Windows

1. 打开“Windows 服务”对话框（**开始 > 设置 > 控制面板 > 管理工具 > 服务**）。
2. 鼠标右键单击 Websense 服务的名称，然后选择**停止**或**启动**。

Linux

当您在 Linux 计算机上使用此程序时，所有服务会一起停止或启动。

1. 转至 **/opt/Websense** 目录。
2. 使用下列命令检查 Websense 服务的状态：
   - `./WebsenseAdmin status`
3. 使用下列命令来停止、启动或重新启动 Websense 服务：
   - `./WebsenseAdmin stop`
   - `./WebsenseAdmin start`
   - `./WebsenseAdmin restart`

> **警告**
> 请勿使用 **kill** 命令来停止 Websense 服务，它可能会对服务造成损坏。

警报

相关主题：

- *溢出控制*，第 239 页
- *配置常规警报选项*，第 240 页
- *配置系统警报*，第 241 页
- *配置类别使用警报*，第 242 页
- *配置协议使用警报*，第 243 页

要促进 Websense 软件和客户端 Internet 活动的追踪和管理，超级管理员可以进行配置，在事件出现时发送警报。

- **系统警报**：关于订购状态和主数据库活动的通知。
- **使用警报**：当出现特定类别或协议到达配置的阈值时将发出通知。

警报可通过电子邮件、屏幕上弹出式消息（Windows **net send** 消息传送）、或 SNMP 消息向选定的收件人发送。

注意

不可向 Linux 计算机发送屏幕弹出式警报。但是，可以从运行 Policy Server 的 Linux 计算机上向 Windows 计算机发送这种警报，只要这台 Linux 计算机上安装了 Samba 客户端即可。请参阅*部署指南*。

对于 Websense 定义和自定义的类别与协议都可以生成使用警报。

溢出控制

相关主题：

- *警报*，第 239 页
- *配置常规警报选项*，第 240 页
- *配置类别使用警报*，第 242 页
- *配置协议使用警报*，第 243 页

使用警报设有内置控制，以避免生成过多的警报消息。使用**每个使用类型的每日最大警报数**设置可指定针对特定类别和协议的用户请求可发送的警报数量限制。请参阅*配置常规警报选项*，第 240 页，以了解更多信息。

您还可以在每个类别和协议使用警报中使用阈值限制。例如，当您将特定类别的阈值限制设置为 10 时，当该类别出现 10 次 （由任意客户端组合所提出的）请求后会生成警报。请参阅*配置类别使用警报*，第 242 页和*配置协议使用警报*，第 243 页，以了解更多信息。

假如每日最大警报数设置为 20 次，而类别警报阈值为 10。管理员只有在出现类别请求超出阈值的前 20 次情况中会接到警报。这意味着只有前 200 次发生的事件会出现在警报消息之中 （阈值 10 乘以警报限制 20）。

配置常规警报选项

相关主题：

- *警报*，第 239 页
- *配置系统警报*，第 241 页
- *配置类别使用警报*，第 242 页
- *配置协议使用警报*，第 243 页

Websense 软件可以将不同类型的系统事件通知管理员，如主数据库类别和订购事宜的更新，以及超出所定义阈值的 Internet 使用。

使用**设置 > 警报和通知 > 警报**页面可选择和配置想要的通知方法，如下所述。然后，利用设置 > 警报和通知部分中的其他页面启用您希望接收的警报。

1. 在**每个使用类型的每日最大警报数**字段中输入一个数，以限制每个类别和协议使用警报的每日生成警报总数。

   例如，您可以将使用警报配置为当有人每 5 次 （阈值）请求访问一个 “体育”类别的站点时即发送。根据用户数量及其 Internet 使用模式，每天可能会生成数百条警报消息。

   如果您输入 10 作为每个使用类型的每日最大警报数，“体育”类别每天最多只会生成 10 条警报消息。在本例中，这些消息会对 “体育”类站点的前 50 次请求提出警报 （每次警报 5 次请求乘以 10 次警报）。

2. 勾选**启用电子邮件警报**复选框，通过电子邮件发送警报和通知。然后，配置电子邮件设置。

SMTP 服务器 IP 或名称	发送电子邮件警报时经由的 SMTP 服务器 IP 地址或名称。
发件人电子邮件地址	用作电子邮件警报发件人的电子邮件地址。
管理员电子邮件地址 (至)	电子邮件警报之主要收件人的电子邮件地址。
收件人电子邮件地址 (抄送)	最多 50 个附加收件人的电子邮件地址。每个地址必须单独占一行。

3. 勾选**启用弹出式警报**复选框，在特定计算机上显示弹出式消息。然后，输入最多 50 个**收件人**的 IP 地址或计算机名称，每个各占一行。

> **注意**
> 不可向 Linux 计算机发送弹出式警报。但是，可以从运行 Policy Server 的 Linux 计算机上向 Windows 计算机发送这种警报，只要这台 Linux 计算机上安装了 Samba 客户端即可。请参阅*部署指南*。

4. 勾选**启用 SNMP 警报**复选框，通过安装在您网络中 SNMP Trap 系统发送警报消息。然后，提供关于您的 SNMP Trap 系统的消息。

社区名称	您的 SNMP Trap 服务器中的 trap 社区名称。
服务器 IP 或名称	SNMP Trap 服务器的 IP 地址或名称。
端口	SNMP 消息所使用的端口号。

5. 在完成后，请单击**确定**以缓存您的更改。直到您单击**全部保存**之后，更改才会生效实施。

配置系统警报

相关主题：

- *警报*，第 239 页
- *配置常规警报选项*，第 240 页
- *查看当前系统状态*，第 245 页

Websense Manager 会通过**状态 > 警报**（详细信息）页面显示详细的系统运行状况与状态信息，如*查看当前系统状态*，第 245 页中所述。

为了确保管理员能够接到重要系统事件的通知（如数据库下载失败或订购即将过期），当其未登录 Websense Manager 时，请将 Websense 系统警报配置为通过电子邮件、弹出式消息、或通过您的 SNMP Trap 系统发送。

在“设置”选项卡中利用**警报和通知 > 系统**页面可选择用于向 Websense 管理员发送警报的方法，以及发送哪些警报。

1. 勾选每种警报将采用的发送方法。根据在“警报”页面中启用的方法，您可以选择**电子邮件**、**弹出式**，以及 **SNMP** 方法。

> **注意**
> 除了生成警报之外，主数据库下载失败和超出订购级别的信息也会记录在 Windows 事件查看器（仅限 Windows）和 Websense.log 文件（Windows 与 Linux 均可用）中。

可生成警报的事件包括：

- 您的订购在一个星期后过期。
- 支持 Search Filtering 的搜索引擎已变更。
- Websense 主数据库下载失败。
- 已从主数据库中添加或删除一个类别或协议。
- 当前用户数量超过了订购级别。
- 当前用户数量达到了订购级别的 90%。
- 您的订购在一个月后过期。
- Websense 主数据库已更新。

2. 在完成后，请单击**确定**以缓存您的更改。直到您单击**全部保存**之后，更改才会生效实施。

配置类别使用警报

相关主题：

- *警报*，第 239 页
- *溢出控制*，第 239 页
- *配置常规警报选项*，第 240 页
- *添加类别使用警报*，第 243 页

当特定 URL 类别的 Internet 活动到达定义阈值时，Websense 软件可以向您发送通知。您可以为类别中被允许或被阻止的请求来定义警报。

例如，您可能希望就针对“购物”类别中站点的每 50 次请求允许即发送一次警报，以帮助确定是否要对该类别设置限制。或者，您可能希望就针对“娱乐”类别中站点的每 100 次请求阻止即接收一次警报，以了解用户是否适应了新的 Internet 使用策略。

在“设置”选项卡中，使用**警报和通知 > 类别使用**页面可查看已建立的警报，以及添加或删除使用警报类别。

1. 查看**允许的类别使用警报**和**已阻止的类别使用警报**列表，以了解哪些类别已配置了警报、每种警报的阈值，以及所选的警报模式。
2. 单击适当列表下方的**添加**，打开“添加类别使用警报”页面（请参阅*添加类别使用警报*，第 243 页）并配置额外的 URL 类别以进行警报。
3. 勾选您希望从其列表中删除的任何类别的复选框，然后单击适当列表下方的**删除**。
4. 在完成之后，单击**确定**以缓存您的更改并返回“类别使用”页面。直到您单击**全部保存**之后，更改才会生效实施。

添加类别使用警报

相关主题：

- *警报*，第 239 页
- *配置常规警报选项*，第 240 页
- *配置类别使用警报*，第 242 页

当您在 “类别使用警报”页面中单击 “添加”时，**添加类别使用警报**页面即会出现。您可在此选择使用警报的新类别、为警报设立阈值并选择警报的方式。

1. 勾选要添加至同一阈值和警报模式的每个类别旁边的复选框。

   注意
   您不能为不可被日志记录的任何类别添加使用警报。请参阅*配置 Filtering Service 以进行日志记录*，第 257 页。

2. 选择导致生产警报的请求数量，以设置**阈值**。
3. 为这些类别勾选每种想要的警报方法的复选框 （**电子邮件**、**弹出式**、**SNMP**）。

   只有在 “警报”页面中已启用的警报方法 （请参阅*配置常规警报选项*，第 240 页）才可进行选择。
4. 单击**确定**以缓存您的更改，然后返回 “类别使用警报”页面 （请参阅*配置类别使用警报*，第 242 页）。直到您单击**全部保存**之后，更改才会生效实施。

配置协议使用警报

相关主题：

- *警报*，第 239 页
- *溢出控制*，第 239 页
- *配置常规警报选项*，第 240 页
- *添加协议使用警报*，第 244 页

当特定协议的 Internet 活动到达定义阈值时，Websense 软件可以向您发送通知。您可以对选中的协议定义允许请求或阻止请求的警报。

例如，您可能希望就针对特定即时消息协议中每 50 次允许请求即发送一次警报，以帮助确定是否要对该协议设置限制。或者，您可能希望就针对特定对等文件共享协议中每 100 次请求阻止即接收一次警报，以了解用户是否适应了新的 Internet 使用策略。

在 “设置” 选项卡中，使用**警报和通知 > 协议使用警报**页面可查看已建立的警报，以及添加或删除使用警报协议。

1. 查看**允许的协议使用警报**和**已阻止的协议使用警报**列表，以了解哪些协议已配置了警报、每种警报的阈值，以及所选的警报模式。
2. 单击适当列表下方的**添加**，打开 “添加协议使用警报” 页面 （请参阅*添加协议使用警报*，第 244 页）并配置额外的协议以进行警报。
3. 选择您希望删除的任何协议的复选框，然后单击适当列表下方的**删除**。
4. 在完成之后，单击**确定**以缓存您的更改并返回 “协议使用警报” 页面。直到您单击**全部保存**之后，更改才会生效实施。

添加协议使用警报

相关主题：

- *警报*，第 239 页
- *配置常规警报选项*，第 240 页
- *配置协议使用警报*，第 243 页

使用**协议使用警报 > 添加协议使用警报**页面可使用警报选择新的协议，为这些警报设立阈值，以及选择警报方法。

1. 勾选要添加至同一阈值和警报模式的每个协议旁边的复选框。

   注意

   除非已配置为要记录入一项或多项筛选器，否则您不能选择对协议进行警报。

   协议警报只能显示由记录协议的协议筛选器所管理的客户端的使用情况。

2. 选择导致生产警报的请求数量，以设置**阈值**。
3. 为这些协议选择每种想要的警报方式 （**电子邮件**、**弹出式**、 **SNMP**）。

   只有在 “警报” 页面中已启用的警报方法 （请参阅*配置常规警报选项*，第 240 页）才可进行选择。
4. 单击**确定**以缓存您的更改，然后返回 “协议使用警报” 页面 （请参阅*配置协议使用警报*，第 243 页）。直到您单击**全部保存**之后，更改才会生效实施。

查看当前系统状态

使用**状态 > 警报**页面找到关于影响您的 Websense 软件运行状况问题的信息，获取排除故障帮助，并查看 Websense 主数据库近期实时更新的详情。

活动警报列表将显示所监视 Websense 软件组件的状态。

- 要了解被监视组件的详细信息，请单击警报消息列表上方的**监视对象？**。
- 要排除故障，请单击错误或警报消息旁边的**解决方案**按钮。
- 要隐藏一个警报消息，请单击**高级**。如果您的机构中不使用 Log Server、Network Agent、或 User Service，或者您不打算启用 WebCatcher，请勾选复选框以隐藏相关的警报。在完成后，请单击**确定**以实施您的更改。

  再次单击**高级**以隐藏高级选项。

实时数据库更新列表向 Websense 主数据库提供紧急更新信息，会显示：

- 更新出现时间
- 更新类型
- 新数据库版本号
- 更新原因
- 接受更新的 Filtering Service 实例的 IP 地址

这些附加更新将出现在定期计划的主数据库更新之外，例如，可用于对暂时分类错误的站点进行重新分类。 Websense 软件每小时检查一次数据库更新。

对于 Websense Web Security 用户，警报页面中还包括第三个列表：**实时安全更新**。该列表与 “实时数据库更新”列表格式相同，但是专门显示与安全相关的数据库更新。

安全更新创建后应立即安装，这样可有效消除漏洞，以防止新的网络钓鱼 （身份欺诈）骗局、流氓应用程序或恶意代码感染主流网站或应用程序。

关于 “实时安全更新”的更多信息，请参阅*实时安全更新* ™，第 29 页。

使用页面上方的**打印**按钮可打开带有 “警报”区域可打印版本的次级窗口。使用浏览器选项可打印此页面，这样可跳过 Websense Manager 主要窗口中的所有导航选项。

备份并还原您的 Websense 数据

相关主题：

- *计划备份*，第 248 页
- *运行立即备份*，第 249 页
- *维护备份文件*，第 249 页
- *还原您的 Websense 数据*，第 250 页
- *中止计划的备份*，第 251 页
- *命令参考*，第 251 页

Websense 备份实用程序使您可轻松备份 Websense 软件设置及策略数据，以及还原至之前的配置。由实用程序储存的数据还可以用于在升级后导入 Websense 配置信息。

备份实用程序会保存：

- 全局配置信息，包括储存在 Policy Database 中的客户端和策略数据。
- 局部配置信息，例如分别储存在各自 Policy Server 中的 Filtering Service 和 Log Server 设置。
- Websense 组件初始化和配置文件。

备份流程运作如下：

1. 由您启动立即备份 （请参阅*运行立即备份*，第 249 页）或定义一个备份计划 （请参阅*计划备份*，第 248 页）。
   - 随时手动启动备份。
   - 当您运行或计划备份时，备份文件将储存在您指定的目录下。
2. 备份实用程序会检查计算机上的所有 Websense 组件、收集符合备份资格的数据，并创建存档文件。文件名格式如下：

   `wsbackup_yyyy-mm-dd_hhmmss.tar.gz`

   此处，*yyyy-mm-dd_hhmmss* 表示备份的日期和时间。**tar.gz** 是可移动压缩文件格式。

   只有根 （Linux）和管理员组的成员 （Windows）才能访问备份文件。

在含有 Websense 组件的每台计算机上运行 Websense 备份实用程序。该工具将识别并保存在当前计算机上找到的下列任何文件：

路径	文件名
\Program Files\Websense\bin *或* **/opt/Websense/bin**	authserver.ini BrokerService.cfg config.xml eimserver.ini LogServer.ini netcache.conf securewispproxy.ini transid.ini upf.conf websense.ini WebUI.ini wsauthserver.ini wscitrix.ini WSE.ini wsedir.ini wsradius.ini wsufpserver.ini
bin/i18n	i18n.ini
bin/postgres/data	postgresql.conf pg_hba.conf
BlockPages/*/Custom	全部自定义阻止页面设置
tomcat/conf/Catalina/Localhost	mng.xml
Windows\system32	isa_ignore.txt
Windows\system32\bin	ignore.txt
/etc/wsLib	wsSquid.ini

在安全的位置保存 Websense 备份文件。这些文件应当是贵组织定期备份程序的一部分。

要还原至较早配置：

1. 从其储存站点中获取备份文件。
2. 将每个备份文件复制至该文件被创建的 Websense 计算机中。
3. 在还原模式下运行备份实用程序。

重要

请始终使用备份实用程序来还原 Websense 软件配置。不要使用其他提取实用程序来从文档中提取文件。

如果备份文件已损坏，则将无法还原您的设置。

在还原流程中，任何错误消息或警告都会显示在运行还原的计算机上。

计划备份

相关主题：

- *运行立即备份*，第 249 页
- *维护备份文件*，第 249 页
- *还原您的 Websense 数据*，第 250 页
- *中止计划的备份*，第 251 页
- *命令参考*，第 251 页

要计划备份，请打开命令窗口并转至 Websense 的 bin 目录（默认为 **C:\Program Files\Websense\bin** 或 **opt/Websense/bin**）。输入下列命令。

```
wsbackup -s -t "<m> <h> <day_of_month> <month>
   <day_of_week>" -d <directory>
```

请注意，时间信息会使用 **crontab** 格式，并需要采用引号和空格。

在范例中显示变量的位置提供下列信息：

变量	信息
<m>	0 - 59 指定开始备份的准确分钟数。
<h>	0 - 23 指定在一天当中开始备份的常规小时数。
<day_of_month>	1 - 31 指定执行备份的日期。如果您计划在 29 至 31 号期间进行备份，实用程序会在不包含该日期的月份中为操作系统采用标准替代程序。
<month>	1 - 12 指定执行备份的月份
<day_of_week>	0 - 6 指定一周中的星期几。 0 代表星期日。

每个字段中可以包含一个数、一个星号、或一个参数列表。请参阅任何 **crontab** 参考内容以了解详细信息。

运行立即备份

相关主题：

- *计划备份*，第 248 页
- *维护备份文件*，第 249 页
- *还原您的 Websense 数据*，第 250 页
- *中止计划的备份*，第 251 页
- *命令参考*，第 251 页

要启动立即备份，打开命令窗口并转至 Websense 的 bin 目录（默认为 **C:\Program Files\Websense\bin** 或 **opt/Websense/bin**）。输入下列命令。

```
wsbackup -b -d <目录>
```

此处，*目录*指备份存档的目的地目录。

警告

请勿在 Websense **bin** 目录下储存备份文件。该目录会在您卸载 Websense 软件时被删除。

当您启动立即备份时，计算机运行备份期间所出现的任何错误消息和通知都会在控制台上显示。

维护备份文件

相关主题：

- *计划备份*，第 248 页
- *运行立即备份*，第 249 页
- *还原您的 Websense 数据*，第 250 页
- *中止计划的备份*，第 251 页
- *命令参考*，第 251 页

当您进行备份时，备份存档会创建并储存一个配置文件（**WebsenseBackup.cfg**）。这项配置文件会标明：

- 在备份目录下保留备份存档的时限
- 在目录下储存所有备份文件所可能占用的最大磁盘空间

在任何文本编辑器中编辑 **WebsenseBackup.cfg** 文件，以更改以下参数：

参数	值
KeepDays	存档文件在备份目录下保存的天数。默认值为 365。
KeepSize	分配给备份文件的字节数。默认值为 10857600。

超过 **KeepDays** 值的任何文件都会从备份目录中删除。如果超出了所分配的磁盘空间，备份目录下最老的文件会被删除，为新文件腾出空间。

还原您的 Websense 数据

相关主题：

- *计划备份*，第 248 页
- *运行立即备份*，第 249 页
- *维护备份文件*，第 249 页
- *中止计划的备份*，第 251 页
- *命令参考*，第 251 页

再还原 Websense 配置数据时，请确保您对当前计算机上现有的组件进行数据还原。

要启动还原程序，请打开命令窗口并转至 Websense 的 bin 目录（默认为 **C:\Program Files\Websense\bin** 或 **opt/Websense/bin**）。输入下列命令。

```
wsbackup -r -f archive_file.tar.gz
```

重要

还原程序可能需要几分钟的时间。当进行还原时，请不要停止此流程。

在还原流程进行期间，备份实用程序会停止所有 Websense 服务。如果实用程序无法停止服务，它会向用户发送消息，以手动停止服务。停止服务时必须按*停止和启动 Websense 服务*，第 238 页中所述的顺序进行。

备份实用程序会保存某些用于与第三方集成产品通讯的文件。由于这些文件位于 Websense 目录结构之外，您必须将每个文件复制至正确的目录下来进行手动还原。

必须手动还原的文件包括：

文件名	还原至
isa_ignore.txt	**Windows\system32**
ignore.txt	**Windows\system32\bin**
wsSquid.ini	**/etc/wsLib**

中止计划的备份

相关主题：
- *计划备份*，第 248 页
- *运行立即备份*，第 249 页
- *维护备份文件*，第 249 页
- *还原您的 Websense 数据*，第 250 页
- *命令参考*，第 251 页

要清空备份计划并停止运行当前的计划备份，打开命令窗口并转至 Websense 的 bin 目录 （默认为 **C:\Program Files\Websense\bin** 或 **opt/Websense/bin**）。输入下列命令：

```
wsbackup -u
```

命令参考

相关主题：
- *计划备份*，第 248 页
- *运行立即备份*，第 249 页
- *维护备份文件*，第 249 页
- *还原您的 Websense 数据*，第 250 页
- *中止计划的备份*，第 251 页

只有根 (Linux) 或管理员组的成员 (Windows) 才能运行备份实用程序。

要随时查看备份实用程序命令选项的完整列表，请输入：

```
wsbackup -h
```

或

```
wsbackup --help
```

wsbackup 命令设有下列选项：

- -b *或* --backup
- -d *directory_path* *或* --dir *directory_path*
- -f *full_file_name* *或* --file *full_file_name*
- -h *或* --help *或* -?
- -r *或* --restore
- -s *或* --schedule
- -t *或* --time
- -u *或* --unschedule
- -v *或* --verbose [0...3]

13 报告管理

相关主题：

- *规划您的配置*，第 254 页
- *管理对报告工具的访问*，第 254 页
- *基本配置*，第 255 页
- *Log Server 配置实用程序*，第 259 页
- *管理日志数据库*，第 271 页
- *配置调查报告*，第 280 页
- *自我报告*，第 284 页

要使用 Websense 演示报告和调查报告，您必须在单台 Windows 服务器上同时安装 Websense Manager 和报告组件。此外，您还必须将 Websense 软件配置为对 Internet 筛选活动进行日志记录。

日志记录将被发送至 Websense Log Server，再由后者将其处理加入必须安装在以下受支持数据库引擎之上的日志数据库中：Microsoft SQL Server Desktop Engine（在本文档中通常称为 MSDE）或 Microsoft SQL Server 企业版或标准版（都称为 Microsoft SQL Server）。关于如何安装这些报告组件的详细信息，请参阅 Websense *安装指南*。

在生成报告时， Websense Manager 将根据您为报告定义的筛选器来显示由日志数据库提供的信息。

以在 Linux 服务器上安装 Websense Manager 或倾向于用 Linux 来满足其报告需求的组织可单独安装 Websense Explorer for Linux 产品来生成报告。该产品将独立于 Websense Manager 运行。请参阅 Websense 的 *Explorer for Linux 管理员指南* 以了解有关安装和使用该程序的说明。

规划您的配置

根据您的网络中 Internet 流量规模的不同，日志数据库可能会变得非常庞大。若想为贵组织制定一套有效的日志记录和报告策略，请仔细思考以下问题：

- 网络流量什么时候最大？

  请考虑将资源密集型的数据库作业和报告作业安排在流量较低的时间。这能提高峰值期间的日志记录和报告效率。请参阅*配置 Internet 浏览时间选项*，第 274 页和*配置日志数据库维护选项*，第 276 页。

- 为支持历史报告，需保留多长时间的数据？

  考虑在数据达到此时限后自动将其删除。这能减小日志数据库所需的磁盘空间。请参阅*配置日志数据库维护选项*，第 276 页。

- 到底需要多详细的信息？

  仔细思考应激活哪些日志记录选项：记录完整 URL 和点击量将增加日志数据库的大小。要减小日志数据库的大小，请考虑：

  - 禁用完整 URL 记录 （请参阅*配置完整 URL 记录*，第 273 页）
  - 记录访问量而不是点击量请参阅 （*配置日志缓存文件*，第 263 页）
  - 启用合并请参阅 （*配置合并选项*，第 265 页）
  - 启用选择类别记录请参阅（*配置 Filtering Service 以进行日志记录*，第 257 页）

要实现成功的报告部署，硬件必须满足或超出保留历史数据所需的预期负荷。

管理对报告工具的访问

当 Websense Manager 与报告组件安装在同一 Windows 服务器上时，报告选项将显示在 Websense Manager 和 Log Server Configuration 实用程序内。

在安装报告组件时，Log Server 将连接至指定的 Policy Server。在登录并访问报告功能期间，您必须选择该 Policy Server。如登录至其他 Policy Server，则您将无法访问 “主要”选项卡上的演示报告或调查报告，或设置选项卡的整个报告部分。

在只使用 WebsenseAdministrator 帐户来登录的组织中，每个使用 Websense Manager 的用户都能访问 Websense Manager 中的全部报告选项，包括演示报告、调查报告和报告工具设置。

在使用委派管理的组织中，对 Websense Manager 中报告工具的访问将由 WebsenseAdministrator 和超级管理员角色的成员来共同控制。在创建角色时，超级管理员将指定该角色是否能访问特定的报告选项。

关于配置报告工具访问的更多信息，请参阅*编辑角色*，第 213 页。

Log Server Configuration 实用程序可通过 Windows 开始菜单来访问。只有那些能访问安装计算机的用户才能打开此实用程序并修改 Log Server 设置。请参阅 *Log Server 配置实用程序*，第 259 页。

如果贵组织的 Websense Manager 是安装在 Linux 服务器上的，或已选择 Websense Explorer for Linux 报告程序而不是在 Windows 平台上运行的报告组件，则报告选项将不会在 Websense Manager 中显示。在“今天和历史”页面上也不会显示 Internet 筛选图表。关于安装和使用该程序来生成报告的信息，请参阅 *Explorer for Linux 管理员指南*。

基本配置

相关主题：

- *配置 Filtering Service 以进行日志记录*，第 257 页
- *指定类别的风险级别*，第 256 页
- *配置报告首选项*，第 257 页
- *Log Server 配置实用程序*，第 259 页
- *管理日志数据库*，第 271 页

您可以使用各种配置选项来自定义自己的报告。

Websense 主数据库将类别划分为不同的**风险级别**。风险级别表明了该类型中的站点可能存在的漏洞类型或级别。您可以使用设置选项卡中的“常规”>“风险级别”页面来自定义贵组织的风险级别。请参阅*指定类别的风险级别*，第 256 页。

您可以使用设置选项卡中的报告 > 首选项页面来配置用于分发报告的电子邮件服务器及激活自我报告功能。请参阅*配置报告首选项*，第 257 页。

日志记录指的是将与 Websense 筛选活动相关的信息存入日志数据库，以便您能生成报告的过程。

您可以使用设置选项卡的常规 > 记录页面来启用日志记录、选择要记录的类别和确定要记录哪些用户信息。请参阅*配置 Filtering Service 以进行日志记录*，第 257 页以了解更多信息。

您可以使用 Log Server Configuration 配置实用程序来管理对日志记录的处理方式以及至日志数据库的连接。请参阅 *Log Server 配置实用程序*，第 259 页，以了解更多信息。

使用“设置”选项卡的“报告”>“日志数据库”页面可管理日志数据库，包括 Internet 浏览时间控制、数据库分区选项和错误日志。请参阅*管理日志数据库*，第 271 页以了解更多信息。

指定类别的风险级别

相关主题：

- *风险级别*，第 36 页
- *阻止页面*，第 73 页
- *使用报告以评估筛选策略*，第 81 页

Websense 主数据库将类别划分为不同的**风险级别**。风险级别表明了该类型中的站点可能存在的漏洞类型或级别。

风险级别主要用于报告之中。“今天”和 “历史”页面中提供按风险级别来追踪的 Internet 活动图表，而且您还可以生成按风险级别排列的演示报告或调查报告。

无限制超级管理员可在**设置 > 风险级别**页面中查看或更改各个风险级别中包含哪些类别。例如，某些公司可能会认为用户自行发布视频的站点属于法律责任、网络带宽损失和生产力损失的风险级别，但如果贵公司需对特定人口统计进行市场调查，您可能会认为这些网站应属于 “商业使用”风险级别。

注意

对安全风险级别默认类别中的需阻止站点，将显示安全阻止页面。对安全风险级别中类别进行的更改将影响报告，但不会影响阻止页面。请参阅*阻止页面*，第 73 页。

Websense 报告中的风险级别信息将反映出您在该页面中所作的分配。

1. 在**风险级别**列表中选择一项。
2. 查看**类别**列表以了解该风险级别目前包括哪些类别。

   当前属于选定风险级别的类别将以勾选标记来表示。而蓝色的 W 图标表示该类别默认属于该风险级别。
3. 您可以通过选定或取消选择类别树上的项来将类别包括在选定的风险级别中或排除在选定的风险级别之外。类别可属于多个风险级别。

   其他选择包括：

选项	描述
全选	选择树上的所有类别。
全部清除	取消选择树上的所有类别。
还原默认设置	将选定风险级别的类别选择重置为 Websense 软件提供的那些。蓝色的 W 图标表示默认分类。

4. 对每个风险级别重复此流程。
5. 单击**确定**以缓存您的更改。直到您单击**全部保存**之后，更改才会生效实施。

配置报告首选项

相关主题：

- *自我报告*，第 284 页
- *计划演示报告*，第 94 页
- *计划调查报告*，第 117 页

当您安排稍晚或重复运行演示或调查报告时，报告将通过电子邮件来分发予指定的收件人。使用“设置”选项卡中的**报告 > 首选项**页面可提供这些电子邮件消息的关键信息。

此页面还可以用来启用自我报告，该功能将使个人用户能够生成关于自己 Internet 活动的调查报告。

1. 通过电子邮件来分发计划的报告时，请输入将出现在发件人字段中的**电子邮件地址**。
2. 输入在通过电子邮件来分发计划的报告时所用电子邮件服务器的 **SMTP 服务器 IP 或名称**。
3. 选中**允许自我报告** 选项框可允许贵组织中的最终用户访问 Websense Manager 并生成关于他们个人 Internet 活动的调查报告。请参阅*自我报告*，第 284 页。
4. 单击**立即保存**以实施您的更改。

配置 Filtering Service 以进行日志记录

相关主题：

- *日志数据库概述*，第 270 页
- *Log Server 配置实用程序*，第 259 页

您可以使用“设置”选项卡上的**常规 > 记录**页面来提供向 Log Server 发送日志记录时将使用的 IP 地址和端口。您还可以通过此页面选择 Websense Filtering Service 应将哪些用户信息和 URL 类别发送至 Log Server，以供报告和类别使用警报使用（请参阅*配置类别使用警报*，第 242 页）。

在有多个 Policy Servers 的环境中，应分别配置各个服务器的“常规”>“记录”页面。所有与活动 Policy Server 相关联的 Filtering Services 都会将其日志记录发送至由此页面标识的 Log Server 上。

在使用多个 Policy Server 时请谨记以下准则：

- 如果任一 Policy Server 的 Log Server 的 IP 地址和端口为空，与该 Policy Server 相关联的 Filtering Service 都将无法记录任何流量以供报告或警报使用。

- 每个 Filtering Service 都将按其所连接至的 Policy Server 的设置来记录流量。如果您更改了不同 Policy Server 的用户信息或类别日志记录选择，为与这些不同的 Policy Server 相关联的用户所生成的报告可能会看起来不太一致。

如果您的环境中既包括多个 Policy Server 也包括多个 Log Server，请务必分别登录各个 Policy Server，并检查与其通信的 Log Server 是否正确。

1. 要记录访问 Internet 的计算机的标识信息，请选中**记录 IP 地址**。
2. 要记录访问 Internet 的用户的标识信息，请选中**记录用户名称。**

   注意

   如果您不记录 IP 地址或用户名，则您的报告中将没有用户数据。即所谓的 **匿名日志记录**。

3. 在 **Log Server IP 地址或名称**字段中输入安装 Log Server 的计算机的 IP 地址或名称。

   重要

   如果 Log Server 和 Policy Server 安装在不同的计算机上，则此项可默认为 localhost。在这种情况下，请输入 Log Server 计算机的正确 IP 地址，以能在 “今天” 和 “历史” 页面中显示图表并使用其他报告功能。

4. 输入向 Log Server 发送日志记录时将使用的**端口**号。
5. 单击**检查状态**以确定 Websense Manager 是否能够与特定的 Log Server 进行通讯。

   将出现一条消息，表明连接是否通过测试。更新 IP 地址或计算机名称和端口 （如需要），直到测试成功为止。
6. 单击**选定类别记录**按钮来打开指明哪些类别将进行记录的区域。

   您在此进行的选择将应用到所有活动策略中的所有类别筛选器。

   注意

   如果您禁用了已设置使用警报的类别的日志记录（请参阅*配置类别使用警报*，第 242 页），则不会发送使用警报。

   报告不会包括不进行日志记录的类别的信息。

   a. 您可以根据需要展开或折叠父类别以查找感兴趣的类别。
   b. 并通过选中其选项框来选择要进行日志记录的类别。

      您必须逐一地选择各个类别或取消选择各个类别。且选择父类别并不会自动地选中其子类别。您还可以使用**全部选择**和**全部清除**来协助进行选择。
7. 单击**确定**以缓存您的更改。直到您单击**全部保存**之后，更改才会生效实施。

Log Server 配置实用程序

相关主题：

- *管理对报告工具的访问*，第 254 页
- *基本配置*，第 255 页
- *停止并启动 Log Server*，第 269 页

您可在安装时配置 Log Server 操作的各个方面，包括 Log Server 与 Websense 筛选组件的互动方式。

Log Server 配置实用程序让您在需要时可以更改这些设置，并配置其他关于 Log Server 操作的细节。此实用程序与 Log Server 安装在同一台计算机上。

1. 从 Windows 开始菜单，选择**程序 > Websense > 实用程序 > Log Server 配置**。

   打开 Log Server 配置实用程序。
2. 选择一个选项卡以显示其选项并进行更改。要了解详细说明请参阅：
   - *配置 Log Server 连接*，第 260 页
   - *配置 Log Server 数据库选项*，第 261 页
   - *配置日志缓存文件*，第 263 页
   - *配置合并选项*，第 265 页
   - *配置 WebCatcher*，第 267 页
3. 单击**应用**以保存更改。
4. 使用**连接**选项卡可停止和重新启动 Log Server，从而使更改生效。

重要

完成 Log Server 配置选项卡上的更改之后，请单击**应用**。然后您**必须**停止并重新启动 Log Server 以使更改生效。要避免多次重新启动 Log Server，请完成对 Log Server 配置的所有更改后再重新启动。

配置 Log Server 连接

相关主题：

- *Log Server 配置实用程序*，第 259 页
- *配置 Log Server 数据库选项*，第 261 页
- *配置日志缓存文件*，第 263 页
- *配置合并选项*，第 265 页
- *配置 WebCatcher*，第 267 页
- *停止并启动 Log Server*，第 269 页

Log Server 配置实用程序的**连接**选项卡中包含了创建和维护 Log Server 和 Websense 筛选组件之间连接的选项。

1. 您可接受默认的 **Log Server 输入端口** (55805) 或输入其他可用端口。

   Log Server 和 Filtering Service 之间的通讯将通过该端口进行。此处输入的端口必须与 Websense Manager 中常规 > 记录页面（设置选项卡）上输入的端口相匹配。

2. 请输入小时数作为**用户/组更新间隔**的时间，以指定 Log Server 联系目录服务进行更新的频率。

   Log Server 将联系目录服务以获得在中有记录的用户的更新信息，例如完整用户名和组分配。

   如果用户组别被更改，则下次更新以前，该用户活动将继续与更改前的组一起被写入报告。需要频繁更新目录服务或用户人数众多的组织应考虑将更新用户/组信息的更新频率设置为比默认的 12 小时一次更加频繁。

3. 单击**应用**以保存更改。

4. 使用服务状态区域的按钮可**启动**或**停止** Log Server。按钮的标签将发生变化，以反映您单击它时所执行的操作。

   注意
   Log Server 停止时，无法记录任何互联网访问活动。

   Log Server 配置实用程序中所做的更改必须在您停止并重新启动 Log Server 后才能生效。

配置 Log Server 数据库选项

相关主题：

- *Log Server 配置实用程序*，第 259 页
- *配置 Log Server 连接*，第 260 页
- *设置数据库连接*，第 263 页
- *配置日志缓存文件*，第 263 页
- *配置合并选项*，第 265 页
- *配置 WebCatcher*，第 267 页
- *停止并启动 Log Server*，第 269 页

打开 Log Server 配置实用程序的**数据库**选项卡，配置 Log Server 与配合使用的方式。

1. 从以下选项中选择一个**日志插入方法**。
   - 开放式数据库连接 (ODBC)：利用一个数据库驱动器管理 Log Server 和之间的数据，从而将记录分别插入数据库中。
   - 批量复制程序 (BCP) （*推荐*）：以批为单位将记录插入数据库。该选项比 ODBC 插入更加高效，因此我们推荐使用。

     注意
     只有在 Log Server 计算机上安装 SQL Server Client Tools 后您才可使用 BCP 选项。

2. 单击**连接**按钮可选择以存储来自 Websense 的互联网访问新信息。请参阅 *设置数据库连接*，第 263 页。

   ODBC 数据源名称 (DSN) 和 **ODBC 登录名称**可显示为数据库连接而建立的设置。

3. 如果您在第 1 步选择了 BCP 作为日志插入方法，请设置以下选项。如果您选择了 ODBC 作为日志插入方法，请跳过这一步。

选项	描述
BCP 文件路径位置	存储 BCP 文件的目录路径。此路径必须为 Log Server 可读写的路径。 只有当日志数据库计算机上安装了 Log Server，或 Log Server 计算机上安装了 SQL Server Client Tools 后才可使用该选项。
BCP 文件创建速率	Log Server 关闭一个批处理文件并创建新的批处理文件之前将记录放入其中所花费的最大分钟数。 此设置将与批处理大小设置配合作用。当达到这两个设置其中之一的限制时，Log Server 将创建新的批处理文件。
BCP 最大批处理大小	新批处理文件创建之前的最大日志记录数量。 此设置将与创建速率设置配合使用。当达到这两个设置其中之一的限制时， Log Server 将创建新的批处理文件。

4. 设置允许的**最大连接数**将指明 Log Server 和数据库引擎之间可创建的内部连接数量。选项是否可用取决于所使用的数据库引擎。
   - **MSDE**：该值被预设为 4，且不可更改。
   - **SQL Server**：请设置 4 至 50 之间的一个数字，以使其可适用于您的 SQL Server 许可证。最小连接数取决于您所选择的日志插入方法。

   > **注意**
   > 连接数越大，日志记录的处理速度也就越快，但是可能会影响到使用同一 SQL Server 的网络中的其他处理的速度。多数情况下，您应将此连接数量设置为小于 20 的数字，请与您的数据库管理员联系以获得帮助。

5. 选中或取消选中**增强日志记录**可启用或禁用该选项，其作用是控制 Log Server 在停止后恢复记录的方式。

   当此选项未被选中（默认）时， Log Server 在停止后会从最旧日志缓存文件的最初开始进行处理。这样会导致中出现重复项目，但会加速 Log Server 的处理速度。

   当此选项被选中时， Log Server 将追踪它在活动的日志缓存文件中的位置。重新启动后， Log Server 将从被停止处恢复处理进程。增强日志记录会降低 Log Server 的处理速度。

6. 单击**应用**以保存更改，然后停止并重新启动 Log Server（请参阅*停止并启动 Log Server*，第 269 页）。

设置数据库连接

相关主题：

- *配置 Log Server 连接*，第 260 页
- *配置 Log Server 数据库选项*，第 261 页

Log Server 配置实用程序的 “数据库” 选项卡中的**连接** 按钮可使您选择日志数据库以存储自 Websense 传入的互联网访问信息。此功能将在安装过程中自动配置，但您可以在因记录需要更改数据库时对其加以更改。（已经有数据库方可建立连接。）

1. 在 “数据源” 对话框中，选择**计算机数据源**选项卡。
2. 为将用于记录新信息的数据库选择 ODBC 连接。
3. 单击**确定**以显示 SQL Server 登录对话框。
4. 如果**使用可信任连接**选项可用，请确保其在您的环境下设置正确。

   MSDE：取消选中 “可信任连接” 选项。

   SQL Server 用户：请与您的数据库管理员联系以获得帮助。

   注意

   如果您通过一个可信任连接与 SQL Server 进行通讯，您可能需要用可信任的用户名和密码配置一些 Websense 服务。请参阅 Websense *安装指南*以获得详细信息。

5. 请输入创建数据库时使用的**登录 ID** 和**密码**。通常这个登录 ID 和密码与 Log Server 安装和数据库创建时所输入的相同。
6. 在完成此操作并在 Log Server 配置实用程序中完成其他任何更改之后，请通过**连接**选项卡停止并重新启动 Log Server。

配置日志缓存文件

相关主题：

- *Log Server 配置实用程序*，第 259 页
- *配置 Log Server 连接*，第 260 页
- *配置 Log Server 数据库选项*，第 261 页
- *配置合并选项*，第 265 页
- *配置 WebCatcher*，第 267 页
- *停止并启动 Log Server*，第 269 页

配置实用程序的**设置**选项卡可让您管理日志缓存文件创建选项，并指定 Log Server 是否对组成每个被请求网站的独立文件进行追踪，或是仅对网站进行追踪。

1. 在**缓存文件路径位置**字段中输入存储日志缓存文件的路径。默认路径为 **<installation directory>\bin\Cache**。（默认安装目录为 C:\Program Files\Websense\）。
2. **缓存文件创建速率**可表明 Log Server 在关闭日志缓存文件 (**log*n*.tmp**) 并创建新文件前，向其发送互联网访问信息所花费的最大分钟数。

   此设置将与大小设置配合作用。当达到这两个设置其中之一的限制时， Log Server 将创建新的日志缓存文件。
3. **缓存文件最大文件大小**将指定在 Log Server 关闭一个日志缓存文件并创建新文件前，该日志缓存文件可达到的大小。

   此设置将与创建速率设置配合使用。当达到这两个设置其中之一的限制时，Log Server 将创建新的日志缓存文件。
4. 选中**启用访问量**可为每个被访问的网站创建一个日志记录。

   注意

   管理日志数据库大小对于高流量网络十分重要，而启用访问量记录则是控制数据库大小和增长的一种方式。

   当该选项未被选中时，每个生成的 HTTP 请求均会创建一个独立的日志记录，以显示不同的页面元素，例如图形和广告。该选项也被称作记录点击量，其创建的将非常庞大，而且增长十分迅速。

   当该选项被选中后，Log Server 将把创建网页的独立元素（例如图形和广告）合并到单一的日志记录中。

   如果您已安装了 Websense Web Security Gateway，则即使已启用了访问量记录，专用于实时扫描的报告也将总是以点击量的形式来报告实时扫描活动。在这种情况下，由于 Web 筛选报告中包含了被实时扫描阻止的通信，因此此报告中显示的数字将低于实时扫描报告中显示的数字。

   注意

   建议在更改记录访问量和点击量的方法之前先创建一个新的数据库分区。请在 Websense Manager 中查看“报告”>“日志数据库”页面（设置选项卡）以创建一个新的数据库分区。
5. 单击**应用**以保存更改，然后停止并重新启动 Log Server（请参阅*停止并启动 Log Server*，第 269 页）。

配置合并选项

相关主题：

- *Log Server 配置实用程序*，第 259 页
- *配置 Log Server 连接*，第 260 页
- *配置 Log Server 数据库选项*，第 261 页
- *配置日志缓存文件*，第 263 页
- *配置 WebCatcher*，第 267 页
- *停止并启动 Log Server*，第 269 页

使用 Log Server 配置实用程序的**合并**选项卡可启用合并功能并设置合并首选项。

注意

管理日志数据库大小对于高流量网络十分重要，而启用合并功能则是控制数据库大小和增长的一种方式。

合并功能可将共享以下元素的互联网请求进行合并，从而减小日志数据库的大小：

- 域名 （例如：www.websense.com）
- 类别
- 关键字
- 操作 （例如：阻止的类别）
- 用户/工作站

日志数据库较小时报告运行的速度会更快。但是，合并日志数据可能会降低一些详细报告的精确性，因为针对相同域名的独立记录可能会丢失。

重要

启用合并功能可能会降低一些报告数据的精确性，例如互联网浏览时间的计算。

1. 选中**合并日志记录**会启用合并功能，从将多个类似的互联网请求合并成单一的日志记录。

   当该选项未被选中 （默认）时，日志数据库将保留每个互联网请求的完整点击量或访问量详细信息 （取决于您在设置选项卡上的选择，请参阅*配置日志缓存文件*，第 263 页）。这样，所提供的报告将更加详细，但相应的，也将更大。

选中该选项将创建一个包含较少详细信息且更小的日志数据库。

重要

要确保报告一致，请考虑在您启用或禁用合并功能时创建一个新的数据库分区。此外，请确保从具有相同合并设置的分区中生成报告。

如果您已安装了 Websense Web Security Gateway，则即使已启用了合并功能，专用于实时扫描的报告也将总是以独立点击量的形式报告实时扫描活动。在这种情况下，由于 Web 筛选报告中包含了被实时扫描阻止的通信，因此此报告中显示的数字将低于实时扫描报告中显示的数字。

2. **合并时间间隔**可指定要合并的第一次记录和最后一次记录之间间隔的最大时间。

   此数值代表在要组合成一个合并记录的所有记录中，最早和最晚记录之间的最大时间差。

   减少间隔时间可增加报告的间隔频率。增加间隔时间可将合并最大化。请注意，较大的间隔也会增加诸如内存、CPU 和磁盘空间等系统资源的使用量。

   如果您启用了 Websense Manager 中 “报告” > “日志数据库” 页面 （设置选项卡）上的完整 URL 选项，则合并日志记录将包含 Log Server 遇到的第一个匹配站点的完整路径 （最多 255 个字符）。

   例如，假设一位用户访问了以下站点，而且这些站点均被归类为购物类别。

   - www.domain.com/shoeshopping
   - www.domain.com/purseshopping
   - www.domain.com/jewelryshopping

   合并功能将利用完整 URL 活动，在 URL www.domain.com/shoeshopping 下创建单一日志项目。

3. 单击**应用**以保存更改，然后停止并重新启动 Log Server（请参阅*停止并启动 Log Server*，第 269 页）。

配置 WebCatcher

相关主题：

- *Log Server 配置实用程序*，第 259 页
- *配置 Log Server 连接*，第 260 页
- *配置 Log Server 数据库选项*，第 261 页
- *配置日志缓存文件*，第 263 页
- *配置合并选项*，第 265 页
- *配置 WebCatcher*，第 267 页
- *WebCatcher 身份验证*，第 268 页
- *停止并启动 Log Server*，第 269 页

WebCatcher 是一个可选功能，可收集无法识别的 URL 和安全 URL，并将这些 URL 提交至 Websense, Inc. 以便就潜在安全和责任风险以及分类对它们进行分析。（WebCatcher 处理无需提交完整 URL 记录。）而 Websense, Inc. 将查看信息并利用新分类的 URL 来更新 Master Database，从而改善筛选。

选择要发送的 URL 类型，并在 Log Server 配置实用程序的 **WebCatcher** 选项卡上设置文件大小和处理时间。

注意

在具有多个 Log Server 的环境中，WebCatcher 仅可针对其中一个 Log Server 启用。一旦启用 WebCatcher，则为其他 Log Server 实例运行 Log Server 配置工具时，该选项卡将处于不可用状态。

发送至 Websense, Inc. 的信息仅包含 URL，不包含用户信息。

以下示例将图解说明激活 WebCatcher 后将被发送的信息。该示例中的 IP 地址反映的是 URL 主机的地址，而不是请求者的 IP 地址。

```
<URL HREF="http://www.ack.com/uncategorized/" CATEGORY="153"
IP_ADDR="200.102.53.105" NUM_HITS="1" />
```

WebCatcher 数据将通过 HTTP Post 被发送至 Websense, Inc.。您可能需要在您的代理服务器或防火墙上创建角色或进行更改才可允许传出 HTTP 通信。请参阅代理服务器或防火墙文档以了解有关说明。

1. 请选择下列选项之一
   - **是，只向激活 WebCatcher 处理的 Websense** 发送指定的 URL。您必须指明要发送的 URL。继续第 2 步。
   - **否，不向取消 WebCatcher 处理的 Websense** 发送信息。如果您选择该选项，则无需其他项目。

2. 选中**发送未分类的 URL** 可发送在您的日志数据库中找到的所有未分类 URL 列表。

   Websense, Inc. 将分析收到的未分类 URL，并将它们添加至恰当的主数据库类别中。这将为所有的组织提高筛选的精确性。

   > **注意**
   >
   > WebCatcher 不会发送企业内部网站点。这包括所有 IP 地址在 10.xxx.xxx.xxx、172.16.xxx.xxx 和 192.168.xxx.xxx 范围内的站点。

3. 选中**发送安全 URL** 可发送在您的中找到的安全 URL 列表。

   Websense, Inc. 将分析收到的安全 URL 以确定键盘记录程序、恶意网站、网络钓鱼、其他诈骗以及间谍软件类别中站点的活动。

4. 在**选择最能反映您的位置的国家 / 地区**中，选择被记录的大部分活动所在的国家/地区。

5. 选中**保存发送到 Websense 的数据副本**选项可保存被发送至 Websense, Inc. 的数据的副本。

   启用该选项时， WebCatcher 将把数据以未加密 XML 文件的形式保存在 Websense\Reporter 目录中。这些文件将标记以日期和时间。

6. **最大上载文件大小**表明文件在发送至 Websense 前可达到的大小范围 （从 4096 KB 到 8192 KB）。

   请确保您的系统可通过 HTTP Post 发送如此大小的文件。

7. **最小每日开始时间**可设置当天的文件大小尚未达到阈值时 WebCatcher 发送文件的开始时间。

   这将确保您系统中的信息每天至少提交并清空一次。

8. 如果 Log Server 计算机访问互联网时必须验证身份，请单击**身份验证**按钮。

   请参阅 *WebCatcher 身份验证*，第 268 页，以了解显示的**身份验证**对话框的有关信息。

9. 单击**应用**以保存更改，然后停止并重新启动 Log Server（请参阅*停止并启动 Log Server*，第 269 页）。

WebCatcher 身份验证

相关主题：

- *Log Server 配置实用程序*，第 259 页
- *配置 WebCatcher*，第 267 页
- *停止并启动 Log Server*，第 269 页

在您单击 WebCatcher 选项卡上的**身份验证**后将显示 “身份验证”对话框。

1. 如果 Log Server 计算机通过代理服务器访问互联网，请选中**使用代理服务器**选项，然后提供所需信息。

字段	描述
代理服务器名称	请输入 Log Server 访问 Internet 所使用的代理服务器的计算机名称或 IP 地址。
代理服务器端口	请输入代理服务器通讯所使用的端口号。

2. 如果 Log Server 计算机访问互联网必须验证身份，请选中**使用基本身份验证**选项，然后输入身份验证的用户名和密码。
3. 单击**确定**保存更改并返回 WebCatcher 选项卡。

停止并启动 Log Server

相关主题：

- *Log Server 配置实用程序*，第 259 页
- *配置 Log Server 连接*，第 260 页

Log Server 将接收来自 Filtering Service 的信息并将其保存在日志数据库中，以便在生成报告时使用。其作用相当于一项 Windows 服务，通常在安装时就已启动，并会在您每次重新启动计算机时启动。

您在 Log Server 配置实用程序中所做的更改只有当您停止并重新启动 Log Server 后才可生效。您可通过 Log Server 配置实用程序中的“连接”选项卡轻松完成这一操作。

1. 从 Windows 开始菜单，选择**程序 > Websense > 实用程序 > Log Server 配置**。
2. 在**连接**选项卡中，单击**停止**。
3. 稍候几秒钟，然后单击**启动**以重新启动 Log Server 服务。
4. 单击**确定**关闭 Log Server 配置实用程序。

注意

Websense 无法记录 Log Server 停止期间发生的 Internet 访问。

日志数据库概述

相关主题：

- *数据库作业*，第 270 页
- *管理日志数据库*，第 271 页

Log Database 将存储 Internet 活动及相关联 Websense 筛选操作的记录。日志数据库在安装时将创建一个编录数据库和一个数据库分区。

编录数据库将为需要访问的各种 Websense 组件提供单一的连接点：状态页、Log Server、演示报告和调查报告。它包含有数据库分区的支持信息，包括类别名称列表、风险级别定义、用户到组的映射、数据库作业等等。编录数据库还维护有一个包含所有可用数据库分区的列表。

数据库分区可存储 Internet 活动的日志记录。对 MSDE 用户，新的分区将按根据 Websense 软件制定的大小翻转规则来创建。 Microsoft SQL Server 用户可将日志数据库配置为按分区大小和日期间隔来创建新的分区（请参阅*配置翻转选项*，第 272 页）以了解更多信息。

注意

只有在 Websense 软件使用 Microsoft SQL Server 作为数据库引擎时，才能使用基于日期的分区。

当分区是以大小为基础时，所有的输入日志记录都将被插入满足大小规则的最新活动分区中。当分区达到指定的最大大小后，将创建新的分区以供插入新的日志记录。

如分区是基于日期的，则将根据已建立的周期来创建新的分区。例如，假设翻转选项为每月，则新的分区将在收到新一月的记录时马上创建。而输入的日志记录将按日期插入相应的分区中。

数据库分区具有灵活、高效的优势。例如，您可以只基于一个分区来生成报告，从而缩小为查找所需信息而必须加以分析的数据范围。

数据库作业

以下数据库作业将随日志数据库一起安装。SQL Server Agent 必须与数据库引擎（MSDE 或 Microsoft SQL Server）运行在同一台计算机上。

- 提取、转换和加载 (ETL) 作业会持续不断的运行，从 Log Server 接受数据、进行处理然后将之插入数据库分区。要对日志记录进行处理并将之存入日志数据库就必须运行 ETL 作业。
- 数据库维护作业将执行数据库维护任务并保持最优的性能。默认情况下，此作业将在夜间运行。

- Internet 浏览时间 (IBT) 作业将对所收到的数据进行分析，并计算每个客户端的浏览时间。IBT 是资源敏感型数据库作业，对大多数的数据库资源都有影响。默认情况下，此作业将在夜间运行。

在“设置”>“日志数据库”页面中可对这些数据库作业的某些环节进行配置。请参阅*日志数据库管理设置*，第 272 页，以了解更多信息。

在配置维护作业和 Internet 浏览时间作业的开始时间时，请充分考虑系统资源和网络流量情况。这些作业属于资源敏感型作业，会降低日志记录和报告的性能。

管理日志数据库

相关主题：

- *日志数据库管理设置*，第 272 页
- *配置翻转选项*，第 272 页
- *配置 Internet 浏览时间选项*，第 274 页
- *配置完整 URL 记录*，第 273 页
- *配置日志数据库维护选项*，第 276 页
- *配置日志数据库分区创建*，第 277 页
- *配置可用分区*，第 278 页
- *查看错误日志*，第 279 页

管理日志数据库将需要对数据库运行的很多环节进行控制：

- 数据库作业将执行哪些操作，以及它们将于何时运行
- 创建新数据库分区的条件。
- 哪些分区可用于报告。

日志数据库的管理员将获得这些以及其他一些选项。请参阅*日志数据库管理设置*，第 272 页。

超级管理员在创建角色时可指定哪些角色可对日志数据库进行管理。请参阅*编辑角色*，第 213 页。

注意

建议限制拥有更改日志数据库设置权限的管理员人数。

日志数据库管理设置

相关主题：

- *管理日志数据库*，第 271 页

您可以通过 “设置” 选项卡的**报告 > Log Database** 页面来管理日志数据库运行的各个环节。这些选项将被划分为多个逻辑部分，并分别进行说明。

要激活对某个部分的更改，您必须单击该部分的 “立即保存” 按钮。单击**立即保存**将立即记录对该部分的更改 （但没必要同时单击 “全部保存”）。

在页面的顶部将显示活动日志数据库的名称和**刷新**链接。此刷新链接可用来重新显示日志数据库页面中的当前信息。所有未 “立即保存” 的更改都将丢失。

关于如何使用各部分的详细说明，请单击下面的相应链接。

- 数据库翻转选项：*配置翻转选项*，第 272 页。
- 完整 URL 记录：*配置完整 URL 记录*，第 273 页。
- Internet 浏览时间配置：*配置 Internet 浏览时间选项*，第 274 页。
- 维护配置：*配置日志数据库维护选项*，第 276 页。
- 数据库分区创建：*配置日志数据库分区创建*，第 277 页。
- 可用分区：*配置可用分区*，第 278 页。
- 错误日志活动：*查看错误日志*，第 279 页。

配置翻转选项

相关主题：

- *日志数据库管理设置*，第 272 页
- *配置 Internet 浏览时间选项*，第 274 页
- *配置完整 URL 记录*，第 273 页
- *配置日志数据库维护选项*，第 276 页
- *配置日志数据库分区创建*，第 277 页
- *配置可用分区*，第 278 页
- *查看错误日志*，第 279 页

使用 “报告” > “日志” 页面 （设置选项卡）上的**数据库翻转选项**部分可指定您希望 Log Database 在何时创建新的数据库分区 （翻转）。

1. 使用**翻转方式**选项可指定数据库分区将按大小 (MB) 或日期（星期或月）来翻转，具体将取决于所使用的数据库引擎。

MSDE 用户必须使用大小翻转选项：Microsoft SQL Server 用户可以选择大小或日期之一。

- 对基于日期的翻转，请选择**星期**或**月**作为计量单位，并指定在新的数据库分区被创建之前应在当前的分区中保存多少个完整的日历星期或月。
- 对基于大小的翻转，请选择 **MB** 并指定数据库必须达到多少 MB 后才会开始翻转。

  Microsoft SQL Server 用户最多可将大小设置为 204800 MB。

  MSDE 用户必须将大小设置为介于 100 MB 到 1536 MB 之间。

注意

如果翻转在一天内的繁忙时发生，则翻转操作期间的性能可能会有所下降。

为避免这种可能，某些环境会选择将自动翻转的时间设置得很长或将大小设置为最大。然后，他们将定期进行手动翻转来防止自动翻转的发生。请参阅*配置日志数据库分区创建*，第 277 页以了解有关手动翻转的更多信息。

请谨记，我们强烈建议不要将单个分区设置得过大。如果数据未能被划分为多个较小的分区，可能会降低报告性能。

在新的数据库分区被创建后，以其为基础的报告将被自动启用（请参阅*配置可用分区*，第 278 页）。

2. 单击**立即保存**来激活对数据库翻转选项的更改。

配置完整 URL 记录

相关主题：

- *日志数据库管理设置*，第 272 页
- *配置翻转选项*，第 272 页
- *配置 Internet 浏览时间选项*，第 274 页
- *配置日志数据库维护选项*，第 276 页
- *配置日志数据库分区创建*，第 277 页
- *配置可用分区*，第 278 页
- *查看错误日志*，第 279 页

“报告”>“日志数据库”页面（“设置”选项卡）的**完整 URL 记录**部分可用来指定将记录各 Internet 请求中 URL 的哪些部分。

> **注意**
> 管理日志数据库大小对于高流量网络十分重要，禁用完整 URL 记录选项则是控制数据库大小和增长的方式之一。

1. 选中**记录全部被请求站点的完整 URL** 将把完整 URL 记录入日志，包括域名 (www.domain.com) 和特定页面的路径 (/products/productA.html)。

   > **重要**
   > 如要您计划生成实时扫描活动报告，请启用完整 URL 记录（请参阅*实时扫描活动报告*，第 130 页）。否则，即使站点内的单个页面被分至不同类别或包含不同威胁，报告也仅会显示已分类站点的域 (www.domain.com)。

   如果未选中此选项，则将只记录域名。此选项可减小数据库的大小，但能提供的详细信息也较少。

   而记录完整的 URL 会产生更庞大的日志数据库，但能提供更多的详细信息。

   如果您在合并为活动时激活完整 URL 记录，则合并后的记录将包括合并组中第一条记录的完整 URL。请参阅 *配置合并选项*，第 265 页以了解更多信息。

2. 单击**立即保存**来激活对完整 URL 记录选项的更改。

配置 Internet 浏览时间选项

相关主题：

- *日志数据库管理设置*，第 272 页
- *配置翻转选项*，第 272 页
- *配置完整 URL 记录*，第 273 页
- *配置日志数据库维护选项*，第 276 页
- *配置日志数据库分区创建*，第 277 页
- *配置可用分区*，第 278 页
- *查看错误日志*，第 279 页

Internet 浏览时间 (IBT) 报告可供查看用户在 Internet 上所花的时间。一项夜间数据库作业将按照当日收到的新日志记录来计算各客户端的浏览时间。通过“设置”>“日志数据库”页面的 **Internet 浏览时间配置**部分可设置浏览时间选项。

1. 为 IBT 数据库作业选择一个**作业开始时间**。

   该作业所需的时间和系统资源将因每天记录的数据量不同而各异。但最好选择夜间维护作业之外且网速较慢的时间来运行此作业（请参阅*配置日志数据库维护选项*，第 276 页）以最小化对生成报告的影响。

   IBT 是资源敏感型数据库作业，对大多数的数据库资源都有影响。如启用此作业，请设置开始时间，以使它不会干扰数据库系统处理计划的报告和执行其他重要操作的性能。此外，还请对该作业进行监视以确定是否需要性能更优的硬件才能满足所有处理需要。

2. 对**读取时间阈值**请设置读取特定网站的分钟数。

   读取时间阈值可用来定义用于 Internet 浏览时间报告的浏览会话。浏览器一打开就会产生 HTTP 流量，即开始一项浏览会话。在此处所设置的时间范围内，只要还在继续产生 HTTP 流量，会话就会保持打开状态。浏览会话将在此时间结束且已无 HTTP 流量时即被视为关闭。但只要 HTTP 流量一产生，新的浏览会话就会立即开始。

   注意

   应尽可能比面更改读取时间阈值，而且在进行更改后应开始一个新的数据库分区。

   为避免报告中的数据不一致，在生成 IBT 报告时请使用读取时间阈值相同的数据库分区。

   请注意，某些网站会使用自动刷新技术来不断地更新信息。例如滚动显示最新报道的新闻网站。这种刷新会产生新的 HTTP 流量。因此，在打开这类网站时，其每次刷新都会产生一条新的日志记录。由于 HTTP 流量之间不存在间断，因此浏览器会话将不会关闭。

3. 请设置**最后读取时间**值来记录浏览会话结束之前，在读取最后一个网站上所花的时间。

   当 HTTP 流量之间的间断长于读取时间阈值时，会话将结束，而最后读取时间的值将被加入会话时间。

4. 单击**立即保存**来激活对 Internet 读取时间选项的更改。

配置日志数据库维护选项

相关主题：

- *日志数据库管理设置*，第 272 页
- *配置翻转选项*，第 272 页
- *配置 Internet 浏览时间选项*，第 274 页
- *配置完整 URL 记录*，第 273 页
- *配置日志数据库分区创建*，第 277 页
- *配置可用分区*，第 278 页
- *查看错误日志*，第 279 页

使用 “报告” > “日志数据库”页面 （“设置”选项卡）的**维护配置**部分可对数据库处理的某些环节进行控制，例如运行数据库维护作业的时间、将执行的某些任务、删除数据库分区和错误日志。

1. 对于**维护开始时间**，请选择一天中将运行数据库维护作业的时间。

   该作业所需的时间和系统资源将因您在此区域中所选择的任务不同而各异。为最小化对其他活动和系统的影响，最好在网络流量较小且无 IBT 作业运行的时间内运行此作业 （请参阅*配置 Internet 浏览时间选项*，第 274 页）。

2. 选中**自动删除分区**，然后指定多少天 （从 2 到 365）后分区将被删除。

   警告

   在删除分区之后，数据将不可恢复。请参阅*配置可用分区*，第 278 页以了解删除分区的其他方式

3. 选中**启用自动重新索引**，然后选择在每个星期中的哪一天将自动执行该处理任务。

   重新索引对维护数据库的完整性和优化报告速度非常重要。

   重要

   此处理最好在网络较为空闲时进行。重新索引数据库分区是资源密集型操作，而且非常耗时。在此处理期间不应运行任何报告。

4. 选中**删除失败批处理前的天数**，并输入一个介于 0 到 90 之间的天数，所有失败的批处理都将在保存此天数之后被删除。

   如果未选中此选项，则失败批处理将被永久保存，以供将来的处理使用。

   如果日志记录因磁盘空间不足或数据库权限不足而插入数据库失败，则该记录将被标记为**失败批处理**。通常，这些批处理会在夜间数据库维护作业中被成功地重新处理并插入数据库。

但在磁盘空间不足或数据库权限不足问题未得到解决之前，重新处理将不会成功。此外，如果未选中**处理未处理的批处理**，则失败批处理将不会被重新处理。它们将在此处所指定的时间过后被删除。

5. 请选中**处理未处理的批处理**以要求夜间数据库维护作业对所有失败批处理进行重新处理。

   如果未选中此选项，则失败的批处理将不会得到重新处理。它们将在上面所指定的时间过后被删除 （如果有）。

6. 选中**删除错误日志前的天数，**并输入一个介于 0 到 90 之间的天数，数据库错误记录将在保存此天数之后被从编录数据库中删除。

   如果未选中此选项，则错误日志将被永久保存。

7. 单击**立即保存**来激活对维护配置 选项的更改。

配置日志数据库分区创建

相关主题：

- *日志数据库管理设置*，第 272 页
- *配置翻转选项*，第 272 页
- *配置 Internet 浏览时间选项*，第 274 页
- *配置完整 URL 记录*，第 273 页
- *配置日志数据库维护选项*，第 276 页
- *配置可用分区*，第 278 页
- *查看错误日志*，第 279 页

使用 “报告” > “日志数据库” 页面 （“设置” 选项卡）**数据库分区创建**部分可定义新数据库分区的属性，如位置和大小选项。该部分还可用来即时创建分区，而不是等待所计划的翻滚 （请参阅*配置翻转选项*，第 272 页）。

1. 请输入创建新数据库分区的**数据**和**日志**文件所需的**文件路径**。
2. 在**初始化大小**中，设置新数据库分区的**数据**和**日志**文件的初始大小 （从 100 到 204800 MB）。

   Microsoft SQL Server 用户：可接受的范围为 100 - 204800

   MSDE 用户：可接受的范围为 100 - 1500

注意

最佳实践：建议计算一段时间内的平均分区大小。然后，使用该值来更新初始大小。这种方法可最大程度地减少必须对分区进行扩展的次数，并能释放资源来处理数据并将之存入分区。

3. 在**增长**中，设置需要更多空间时分区的**数据**和**日志**文件大小的增长幅度（以 MB 为单位）。

   Microsoft SQL Server 用户：可接受的范围为 1 -999999

   MSDE 用户：可接受的范围为 1 -450

4. 单击**立即保存**以应用所输入的路径、大小和增长更改。

   在进行这些更改之后所创建的分区将使用新设置

5. 单击**立即创建**可在下次 ETL 作业运行时创建新的分区（请参阅*数据库作业*，第 270 页），而不论自动翻转的设置如何。此过程通常需要几分钟。

   为确保新的分区将使用在此部分进行的更改，请务必在单击**立即创建**之前单击**立即保存**。

   定期单击内容窗格中的 “刷新” 链接。完成创建流程之后，“可用分区” 区域将显示新的分区。

配置可用分区

相关主题：

- *日志数据库管理设置*，第 272 页
- *配置翻转选项*，第 272 页
- *配置 Internet 浏览时间选项*，第 274 页
- *配置完整 URL 记录*，第 273 页
- *配置日志数据库维护选项*，第 276 页
- *配置日志数据库分区创建*，第 277 页
- *查看错误日志*，第 279 页

“报告” > “日志数据库” 页面（“设置” 选项卡）的**可用分区**部分将列出可用于报告的全部数据库分区。该列表将显示覆盖的日期，以及各分区的大小和名称。

使用此列表可控制在报告中将包括哪些数据库分区，以及可选择要删除的分区。

1. 对于想要包括在报告中的各个分区，请选中其旁边的**启用**。

   根据需要使用列表上方的**全部选择**和**不选**选项。

   您必须至少启用一个将用于报告的分区。使用**不选**选项可一次禁用所有分区，然后您可只启用其中的少数分区。

   使用这些选项可管理在生成报告时应处理多少数据，并提高报告的处理速度。例如，如果您计划为六月生成一系列的报告，则请取消选择所有不包括六月中日期的分区。

   重要

   此选择将同时影响计划的报告和交互式运行报告。为避免生成没有数据的报告，请确保按计划运行报告时，相关的分区已经启用。

2. 如果不再需要某个分区，请单击位于其名称一侧的**删除**选项。该分区将在下一次夜间数据库维护作业运行时被真正地删除。

   警告
   使用此选项时请小心。已删除的分区将无法恢复。

   删除废旧的分区可最大程度地减少日志数据库中的分区数量，从而提高数据库和报告的性能。使用此“删除”选项可按需要删除单个的分区。如果您希望按计划删除较早的分区，请参阅*配置日志数据库维护选项*，第 276 页。

3. 单击**立即保存**来激活对可用分区选项的更改。

查看错误日志

相关主题：

- *日志数据库管理设置*，第 272 页
- *配置翻转选项*，第 272 页
- *配置 Internet 浏览时间选项*，第 274 页
- *配置完整 URL 记录*，第 273 页
- *配置日志数据库维护选项*，第 276 页
- *配置日志数据库分区创建*，第 277 页
- *配置可用分区*，第 278 页

使用“报告”>“日志数据库”页面（“设置”选项卡）的**错误日志活动**部分可查看在作业于 Websense 日志数据库上运行期间所产生的错误记录（请参阅*数据库作业*，第 270 页）。这些信息在进行故障排除时可能非常有用。

请选择以下选项之一。

- 从下拉列表中选择一个数字，以显示该数量的错误日志项。
- 选择**全部查看**以显示所有错误日志项。
- 选择**不查看**以隐藏所有错误日志项。

配置调查报告

相关主题：

- *数据库连接与报告默认*，第 280 页
- *显示和输出选项*，第 282 页

调查报告将使您能以交互式的方式深入研究贵组织的 Internet 使用情况信息。请参阅*调查报告*，第 100 页。

调查报告主页面上的“选项”链接将使您能有机会修改将用于生成报告的日志数据库。它还让您能够修改详细报告的默认视图。请参阅*数据库连接与报告默认*，第 280 页。

wse.ini 文件将使您能够配置查看摘要和多层次报告的某些默认设置。它还使您能够控制在将报告输出为 PDF 格式文件时的默认页面大小。请参阅*显示和输出选项*，第 282 页。

数据库连接与报告默认

相关主题：

- *配置调查报告*，第 280 页
- *显示和输出选项*，第 282 页
- *摘要报告*，第 101 页
- *多级摘要报告*，第 104 页

使用**调查报告 > 选项**页面可连接所需要的日志数据库，并可控制调查报告详情视图的默认设置。

对此页面所作的更改将只影响您的报告。其他管理员，甚至是登录以生成自我报告的用户，均可为自己的报告活动更改这些值。

1. 请选择将用于调查报告的日志数据库。
   - 选择**查看编录数据库**来连接 Log Server 进行日志记录的日志数据库。继续第 2 步。
   - 要访问其它日志数据库：
     a. 取消**查看编录数据库**选项。

b. 输入以下信息以识别所需的日志数据库。（调查报告可基于 6.3.x 或 v7.0 数据库来生成。）

字段	描述
服务器	输入日志数据库所在计算机的名称或 IP 地址。
数据库	输入日志数据库的名称。
用户 ID	输入拥有该数据访问权限之账户的用户 ID。 如果 Log Server 在安装时被设置为使用可信任连接来访问日志数据库，则请将此留空。 如不确定，则请输入 **sa**。这是 MSDE 的默认用户 ID 和 Microsoft SQL Server 的默认管理员 ID。
密码	输入指定用户 ID 的密码。对可信任连接，请将此留空。

2. 为详细报告选择以下默认设置。

字段	描述
选择调查报告的默认日期范围	选择初始摘要报告显示的日期范围。
选择默认详细报告格式	选择**智能列选择**来按所报告信息的默认列集合显示详细报告。 选择**自定义列选择**来指定所有详细报告在初次显示时的准确列。您可以使用“可用列”列表来进行选择。 用户可在报告生成后对所显示的列进行修改。
选择报告类型	选择是否在初次打开详细报告时显示： • **细节**：每行显示一条记录，可显示时间。 • **摘要**：将共用同一元素的所有记录合并成一项。具体的元素将根据所报告信息的不同而各异。通常，进行摘要的元素将显示在度量之前的最右侧列中。时间将无法显示。
可用列/当前报告	在“可用列”列表中选中列名称，然后单击相应的箭头将之移动至“当前报告”列表中。“当前报告”列表最多可拥有 7 个列。 在“当前报告”列表已包括详细报表在初始显示时的所有列后，可对列的顺序进行设置。选择列表中的一项，然后使用上下箭头按钮来调整它的位置。

3. 单击**保存选项**来立即保存所有更改。

显示和输出选项

相关主题：

- *配置调查报告*，第 280 页
- *数据库连接与报告默认*，第 280 页
- *输出到文件*，第 120 页

您可以对摘要和多层次调查报告中特定报告选择和报告结果的显示方式进行调整，并指定报告在输出为 PDF 格式时的默认页面大小。

这些调查报告配置选项都包含在 **wse.ini** 文件中。其默认位置是

```
C:\Program Files\Websense\webroot\Explorer\wse.ini
```

下面的表格列出了将影响调查报告的显示和输出的参数、它们的作用及默认值。（请勿修改 wse.ini 文件中的任何其他设置。）

参数	描述
maxUsersMenu	数据库的用户数必须小于此值 （默认为 5,000 ）才能在“internet 用户”列表中将用户显示为一项报告选项。
maxGroupsMenu	数据库的组数必须小于此值 （默认为 3,000）才能在“internet 用户”列表中将组显示为一项报告选项。 **请注意**：要在 “internet 用户” 列表中显示组，组的数量就必须达到 2 个或以上。 此外，要在 “internet 用户” 列表中显示域，域的数量也必须达到 2 个或以上。但对域没有最大限值。
maxUsersDrilldown	此参数将与 warnTooManyHits 参数一起来控制 “用户” 选项何时以红色显示。当以红色显示时，选择用户将产生非常大的报告，并会降低报告的生成速度。 如果用户数大于此值 （默认为 5,000）且点击量大于 warnTooManyHits 值，则用户选项将在各种下拉列表和值列表中显示为红色。 如果用户数大于此值，但点击量小于 warnTooManyHits 值，则用户选项将以正常颜色显示，且结果报告的大小也会比较合理。
maxGroupsDrilldown	如果准备生成的报告所包括的组数超过此数值（默认为 2,000）则组选项在下拉列表中将以红色显色。当以红色显示时，选择组将产生非常大的报告，并会降低报告的生成速度。

参数	描述
warnTooManyHits	此参数将与 maxUsersDrilldown 参数一起来控制“用户”选项何时以红色显示。 如果用户数大于 maxUsersDrilldown，但点击量小于此值 （默认为 10,000）则用户选项将*不会*以红色显示。 如果用户数大于 maxUsersDrilldown，且点击量也大于此值，则用户选项将会以红色显示。当以红色显示时，选择用户将产生非常大的报告，并会降低报告的生成速度。
hitsPerPage	此值将决定每页可显示的最大项数 （默认为 100）（这不会影响打印的报告。）
maxOutputBufferSize	此值将决定在调查报告主页面上可显示的最大数据量 （以字节计） 。如果所请求的数据超出了此限值（默认为 4,000,000 或 4MB），则将在报告的尾部以红色显示部分数据尚未显示的消息。 如果有此需要的话，较大的值将使您能在一份报告中显示更多的数据。但若遇到内存问题，则请考虑减小此值。
sendMulti	默认情况下，该选项处于禁用状态 (0)。将之设置为 1 （启用）后，会将极大的计划详细报告分割成多个文件。每个文件 10,000 行。这些同属于一份报告的文件将在压缩后被发送给电子邮件收件人。使用最常见的文件压缩工具即可打开这些报告文件。
maxSlices	此值将决定饼图的最大分区数 （默认为 6），包括一个其他分区，其中将包含所有不属于某个独立分区的值。
timelineCompressionThreshold	此选项将在“群组类似点击/查看所有点击量”选项可用时仅用于按天或者按月的用户活动。报告将把在此处所设的秒数（默认为 10）内发生的全部点击归入同一类别。
PageSize	调查报告的结果可输出为 PDF 格式以便于分发或打印，其页面大小 （默认为 Letter）可以是 • A4 （8.27 X 11.69 英寸） • Letter （ 8.5 X 11 英寸）

自我报告

相关主题：

- *配置报告首选项*，第 257 页
- *访问自我报告*，第 121 页
- *调查报告*，第 100 页

通过自我报告功能，用户可以查看基于他们自己的 Internet 活动的调查报告。这将使他们能查看哪些与他们相关的信息将被收集和监视，而这也是很多国家的政府法规所要求的。此外，查看自己的活动还能促使一些用户开始改变自己的浏览习惯，从而使自己能够满足组织的 Internet 政策。

注意

只有当 Websense Manager 和报告选项都安装在同一 Windows 操作系统上时，才可使用自我报告。请参阅*部署指南*以了解详细信息。

要启用自我报告：

1. 转至**设置 > 常规 > 目录服务**，对专用于验证以自己网络凭据来访问 Websense Manager 的用户的目录服务进行配置。该操作可能在之前启用按用户和组名称进行筛选时已经完成。请参阅*目录服务*，第 54 页。

   如果您的安装包括多个 Policy Server，则您必须分别登录每一个 Policy Server，配置具有相应目录服务信息的“目录服务”页面。
2. 转至**设置 > 报告 > 首选项**，选中**允许自我报告**复选框。请参阅*配置报告首选项*，第 257 页。

启用该选项之后，请务必告知用户生成报告所需的信息：

- 访问自我报告界面的 URL。提醒用户，他们可将该 URL 存入收藏夹或书签中以供将来使用。

  了解与该 URL 相关的详细信息。
- 在登录时应选择哪个 Policy Server。

  在只有一个 Policy Server 的网络中，此项可忽略。如果您的网络拥有多个 Policy Server，则应告知用户可与将对他们的网络登录进行身份验证的目录服务进行通信的 Policy Server 的 IP 地址。这也就是您在安装 Log Server 时指定的 Policy Server。
- 登录时应使用什么用户名和密码。

  自我报告用户在登录时必须输入他们的网络用户名和密码。

访问自我报告界面的 **URL** 是：

```
https://<ServerIP>:9443/mng/login/pages/
   selfReportingLogin.jsf
```

请使用运行 Websense Manager 的计算机的 IP 地址来代替 <ServerIP>。

管理员和用户也可通过打开 Websense Manager 的登录页面并单击 “自我报告” 链接来访问自我报告的登录页面。

如果您的网络拥有**多个 Policy Server**，则必须告知用户在进行自我报告登录时应选择哪个。

14 网络配置

相关主题：

- *硬件配置*，第 288 页
- *Network Agent 配置*，第 289 页
- *验证 Network Agent 配置*，第 295 页

当您以独立模式（未与代理或防火墙产品集成）运行 Websense 软件时，Websense Network Agent 即会启动：

- Internet 内容筛选
- 网络协议和 Internet 应用程序管理
- 带宽管理
- 字节传送记录

在一个集成 Websense 软件部署中，第三方产品负责将用户请求发送至 Websense 软件以作筛选，然后将阻止页面发送回客户端。在此环境下，Network Agent 仍然将被用于筛选非 HTTP 请求、提供增强记录细节或两者同时进行。

而且 Network Agent 将持续监视整体网络使用情况，包括网络上的字节传送，并按预定义的时间间隔将使用摘要发送至 Websense 软件。每个摘要均包括开始时间、结束时间、使用的总体字节数和每个协议使用的字节数。

默认情况下，Network Agent 还会向 Policy Server 提供带宽的使用数据，并向 Filtering Service 提供筛选日志数据

通常，Network Agent 会被配置为可查看网络上的所有通信。它还可区分以下内容：

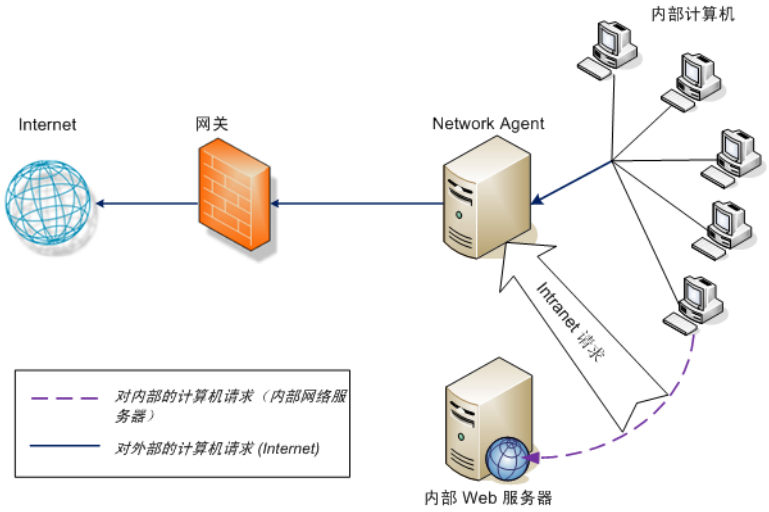
- 从内部计算机发送至内部计算机的请求 （例如，至 Internet 服务器的点击）
- 从内部计算机发送至外部计算机 （如 Web 服务器）的请求 （例如，用户 Internet 请求）

在监视雇员 Internet 使用过程中后者将是优先事宜。

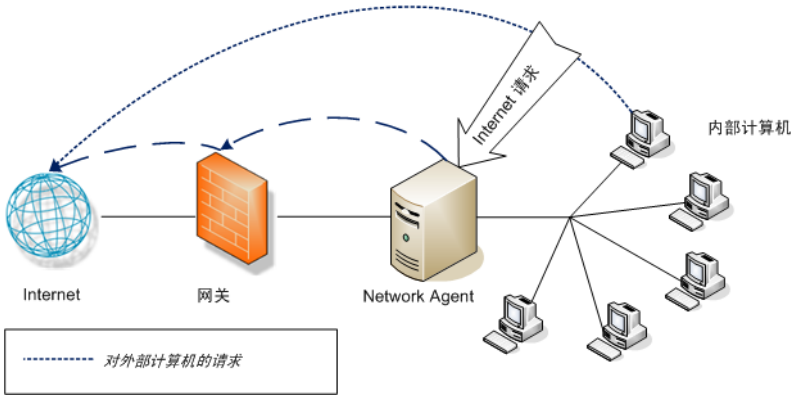
硬件配置

每个 Network Agent 实例将对**来自**被识别为属于您的网络之计算机的通信进行监视。默认情况下，它仅会监视那些被发送**至**您指定的内部计算机（例如，内部 Web 服务器）的通信。

您可自定义被每个 Network Agent 实例监视的内部计算机（网络段），或在一台 Network Agent 计算机上自定义被每个网络接口卡监视的内部计算机（网络段）。



监视发送至内部计算机的请求



监视发送至外部计算机的请求

每个 Network Agent 实例必须：

- 位于网络中的恰当位置，从而可检测来往于所有被监视计算机的通信。
- 至少有 1 个 NIC 专用于监视通信。

可被安装在拥有多个 NIC 的计算机上，并可使用多个 NIC 同时监视请求并发送阻止页面。如果您在 Network Agent 计算机上添加新的 NIC，则需重新启动 Network Agent 服务，然后配置该新 NIC （请参阅*配置 NIC 设置*，第 292 页）。

> **注意**
>
> 要确定 Network Agent 是否可查看一个网络段中的通信，请使用 Network Traffic Detector 实用程序。请参阅*验证 Network Agent 配置*，第 295 页。

有关 Network Agent 部署和 NIC 要求的更多信息，请参阅*部署指南*。

有关配置 Network Agent 以监视内部网络请求、使用特定的 NIC 以及执行增强日志记录的信息，请参阅 *Network Agent 配置*，第 289 页。

Network Agent 配置

相关主题：

- *硬件配置*，第 288 页
- *配置全局设置*，第 290 页
- *配置本地设置*，第 291 页
- *配置 NIC 设置*，第 292 页
- *添加或编辑 IP 地址*，第 294 页

安装 Network Agent 之后，请使用 Websense Manager 以配置它的网络监视操作。 Network Agent 设置分为两个主要区域：

- **全局设置**将对所有的 Network Agent 实例生效。使用这些设置可以：
  - 识别网络中的计算机。
  - 列出网络内 Network Agent 可监视其**传入**请求的计算机（例如，内部 Web 服务器）。
  - 指定带宽计算方法和协议记录行为。
- **本地设置**仅适用于选定的 Network Agent 实例。使用这些设置可以：
  - 识别与每个 Network Agent 相关联的 Filtering Service 实例。
  - 记录该 Network Agent 监视的计算机所使用的代理和缓存。
  - 配置每个网络接口卡 (NIC) 在 Network Agent 计算机上的使用方法（是用于监视请求、发送阻止页面，或是同时用于两者）。

    网卡设置还可以确定每个 Network Agent 实例监视的网络段。

配置全局设置

相关主题：

- *硬件配置*，第 288 页
- *配置本地设置*，第 291 页
- *配置 NIC 设置*，第 292 页
- *添加或编辑 IP 地址*，第 294 页

使用**设置 > Network Agent > 全局**页面可为所有 Network Agent 实例定义监视和记录操作。

内部网络定义列表可识别属于您的网络的计算机。默认情况下，Network Agent 不会监视这些计算机之间的通信 （内部网络通讯）。

系统会按默认提供列表中的初始项集合。您可添加其他项，或者编辑或删除现有项。

要监视的内部通信列表包括了内部网络定义中，您**确实**想要 Network Agent 对其进行通信监视的任何计算机。例如，这其中可能包含内部 Web 服务器，从而可帮助您追踪内部连接情况。

网络内任何地点发送至特定内部计算机的任何请求都将受到监视。默认情况下，该列表为空白。

- 单击**添加**可在相应列表内添加 IP 地址或范围。请参阅*添加或编辑 IP 地址*，第 294 页，以了解更多信息。
- 要编辑列表中的项目，请单击 IP 地址或范围。请参阅*添加或编辑 IP 地址*，第 294 页，以了解更多信息。
- 要从列表中删除项目，请勾选 IP 地址或范围旁边的复选框，然后单击**删除**。

其他设置选项可允许您确定 Network Agent 计算带宽使用的频率、是否记录协议通信，以及记录的频率。

字段	要进行的操作
带宽计算间隔	请输入一个介于 1 和 300 之间的数字以指定计算的间隔时间（单位为秒），Network Agent 将按此间隔计算带宽的使用情况。例如，输入 300，则表明 Network Agent 将每隔 5 分钟就计算一次带宽。 默认设置为 10 秒钟。
定期记录协议流量	勾选此选项以启用记录间隔字段。
记录间隔	请输入一个介于 1 和 300 之间的数字以指定计算的间隔时间（单位为分钟），Network Agent 将按此间隔对协议进行记录。例如，输入 60，则表明 Network Agent 将每隔一小时写入一次日志文件。 默认设置为 1 分钟。

完成更改后，请单击**确定**以缓存更改。直到您单击**全部保存**之后，更改才会生效实施。

配置本地设置

相关主题：

- *硬件配置*，第 288 页
- *配置全局设置*，第 290 页
- *配置 NIC 设置*，第 292 页

使用**设置 > Network Agent > 本地设置**页面可为选定的 Network Agent 实例配置筛选操作、代理信息和其他设置。选定的 Network Agent 实例的 IP 地址将显示在内容窗格的标题栏中，并在左侧导航窗格中突出显示。

使用 **Filtering Service 定义**设置可指定与选定的 Network Agent 实例相关联的 Filtering Service，以及 Filtering Service 不可用情况下对 Internet 请求的回应方式。

字段	要进行的操作
Filtering Service IP 地址	选择与此 Network Agent 相关联的 Filtering Service。
如果 Filtering Service 不可用	选择**允许**以允许所有请求，或选择**阻止**以阻止所有请求，直至 Filtering Service 再次可用。默认选择为 “允许”。

要确保用户请求得到正确的监视、筛选和记录，请使用**代理和缓存**列表来指定与 Network Agent 通讯的任何代理或缓存服务器的 IP 地址。

- 单击**添加**可在列表内添加 IP 地址或范围。请参阅*添加或编辑 IP 地址*，第 294 页，以了解更多信息。
- 要编辑列表中的项目，请单击 IP 地址或范围。
- 要从列表中删除项目，请勾选 IP 地址或范围旁边的复选框，然后单击**删除**。

使用**网络接口卡**列表可配置单个 NIC。单击**名称**栏中的 NIC，然后参阅*配置 NIC 设置*，第 292 页，以获得进一步说明。

如果您网络中的 HTTP 请求需通过非标准端口，请单击**高级 Network Agent 设置**，为 Network Agent 监视提供正确的端口。默认情况下，**用于 HTTP 通信的端口**为 **8080, 80**。

除非 Websense 技术支持有所指示，否则请勿对此部分中的其他设置进行更改。

字段	描述
模式	• 无 （默认） • 常规 • 错误 • 细节 • 带宽
输出	• 文件 （默认） • 窗口
端口	55870 （默认）

完成对 Network Agent 设置的更改后，请单击**确定**以缓存更改。直到您单击**全部保存**之后，更改才会生效实施。

配置 NIC 设置

相关主题：

- *硬件配置*，第 288 页
- *Network Agent 配置*，第 289 页
- *配置 NIC 监视设置*，第 293 页
- *添加或编辑 IP 地址*，第 294 页

使用 **Network Agent > 本地设置 > NIC 配置**页面可指定 Network Agent 通过每个可用网络接口卡 (NIC) 来监视和管理网络使用情况的方式。

NIC 信息可提供您所做更改的上下文，显示 **IP 地址**、简要 NIC **描述**以及卡**名称**。使用此信息可确保您正确配置了 NIC。

监视

在多个 NIC 配置中，您可将其中一个 NIC 确定为监视网络通信，另一个确定为用于阻止页面。至少需有一个 NIC 用于监视，且可有多个 NIC 用于监视通信。

使用**监视**部分可指明是否**使用该 NIC 监视通信**。

- 如果不使用此 NIC 进行监视，请取消选中复选框，然后继续下一部分。
- 如果使用该 NIC 进行监视，请选中复选框，然后单击**配置**，然后您将被转至“配置监视操作”页面。请参阅*配置 NIC 监视设置*，第 293 页，以了解相关说明。

其他 NIC 选项

除了配置监视选项，您还可确定其他 NIC 操作：

1. 通过阻止，可确保合适的 NIC 被列于**阻止 NIC** 字段中。如果您需配置多个 NIC，在每个 NIC 设置的这一字段中均应显示相同的值。换言之，仅有一个 NIC 被用于阻止。
2. 如果您正在**独立**模式下运行 Websense 软件，则**筛选和记录 HTTP 请求**将被选中，且不能更改。
3. 如果您已在 Websense 软件中集成了第三方设备或应用程序，请使用**集成**选项来指明该 Network Agent 进行筛选和记录 HTTP 请求的方式。您的环境中未应用的选项将被禁用。
   - 选择**记录 HTTP 请求**可提高 Websense 报告的精确性。
   - 选择**筛选所有不通过 HTTP 端口发送的请求**可利用 Network Agent 仅对未通过集成产品发送的 HTTP 请求进行筛选。
4. 通过协议管理，可指明 Network Agent 是否应使用此 NIC 来筛选非 HTTP 协议。
   - 选中**筛选非 HTTP 协议请求**可激活协议管理功能。这样将允许 Websense 软件对 Internet 应用程序和数据传送方法进行筛选，例如传送即时消息、流媒体、文件共享、Internet 邮件的方法。请参阅*筛选类别与协议*，第 34 页和*使用协议*，第 156 页，以了解更多信息。
   - 选中**通过协议测量带宽使用情况**可激活 Bandwidth Optimizer 功能。Network Agent 可使用此 NIC 来追踪每个协议或应用程序的网络带宽使用情况。请参阅*使用 Bandwidth Optimizer 来管理带宽*，第 161 页，以了解更多信息。

配置 NIC 监视设置

使用**本地设置 > NIC 配置 > 监视列表**页面可指定 Network Agent 通过选定的网络接口卡 (NIC) 监视的计算机。

1. 在监视列表中指定 Network Agent 监视的请求：
   - **所有**：Network Agent 将监视来自通过选定的 NIC 可查看的所有计算机的请求。通常，这会包括与当前 Network Agent 或 NIC 相同的网络段内的所有计算机。
   - **无**：Network Agent 不监视任何请求。
   - **特定**：Network Agent 仅对 “监视列表”中包含的网络段进行监视。
2. 如果您选择 “特定”，请单击**添加**，然后指定 Network Agent 应监视的计算机的 IP 地址。请参阅*添加或编辑 IP 地址*，第 294 页，以了解更多信息。

> **注意**
> 您输入的 IP 地址范围不可重叠。如果范围重叠，将无法精确测量网络带宽，且基于带宽的筛选可能无法正确进行。

要从列表中删除一个 IP 地址或范围，请选中相应的列表项，然后单击**删除**。

3. 通过 “监视列表例外项”，可确定 Network Agent 不需监视的内部计算机。

   例如，Network Agent 可忽略由 CPM Server 提出的请求。因此，CPM Server 不会导致 Websense 日志数据或任何状态监视输出出现混乱。

   a. 要确定此类计算机，请单击**添加**，然后输入它的 IP 地址。

   b. 重复以上步骤可确定其他此类计算机。

4. 单击**确定**以缓存您的更改，然后转至 “NIC 配置” 页面。直到您单击**全部保存**之后，更改才会生效实施。

添加或编辑 IP 地址

相关主题：

- *配置全局设置*，第 290 页
- *配置本地设置*，第 291 页
- *配置 NIC 设置*，第 292 页

使用**添加 IP 地址**或**编辑 IP 地址**页面可对以下任何 Network Agent 列表进行更改：内部网络定义、要监视的内部通信、代理和缓存、监视列表，或监视列表例外项。

- 添加或编辑一个 IP 地址范围时，请确保该地址范围不与列表中的任何现有项 （单一 IP 地址或范围）有所重叠。
- 添加或编辑一个单一 IP 地址时，请确保其不会包含于列表中已经存在的范围中。

要添加一个新的 IP 地址或范围：

1. 请选择 **IP 地址**或 **IP 地址范围**单选按钮。
2. 请输入一个有效的 IP 地址或范围。
3. 单击**确定**返回前一个 Network Agent 设置页面。新的 IP 地址和范围将显示在相应的表格中。

   要在更改未经缓存的情况下返回前一页面，请单击**取消**。
4. 如有需要，可重复上述步骤添加其他 IP 地址。

编辑一个现有的 IP 地址或范围时，“编辑 IP 地址” 页面将显示选择的项目，而其中对应的单选按钮已被选中。进行任何必要更改，然后单击**确定**返回前一页面。

完成添加或编辑 IP 地址后，请在 “Network Agent 设置” 页面上单击**确定**。直到您单击**全部保存**之后，更改才会生效实施。

验证 Network Agent 配置

在 Websense Manager 中完成 Network Agent 配置后，请使用 Network Traffic Detector 来确保您网络中的计算机可显示在 Websense 软件中。

1. 转至**启动 > 程序 > Websense > 实用程序 > Network Traffic Detector**，启动该工具。
2. 从**网络适配器**下拉列表中选择一个网卡。
3. 检查在**监视的网络范围**列表中显示的地址，以验证所有相应子网络均已在列表中列出。
4. 使用**添加子网络**和**删除子网络**按钮可更改进行测试的网络范围。
5. 单击**开始监视**。

   Network Traffic Detector 可以通过监视计算机通过网络发送的信息来检测网络中的计算机。**检测到的计算机数量**列表可显示被检测到的正在运行的计算机。
6. 要查看被此工具检测到的计算机的特定信息，请在 “监视的网络范围”列表中选择一个子网络，然后单击**查看检测到的计算机**。

   如果特定计算机不在列表中，则表明其正在进行网络通信。要验证这一点，可转至计算机，启动浏览器，然后导航至一个网站。接着返回 Network Traffic Detector 并查看是否该计算机显示在**检测到的计算机**对话框中。
7. 完成网络通信可见性测试后，请单击**停止监视**。

如果某些计算机不可见，则可：

- 查看网络配置和 NIC 部署要求 （请参阅*硬件配置*，第 288 页）。
- 在 Websense 软件的*安装指南*中查看更多有关网络配置的详细信息。
- 验证您已正确配置了监视 NIC （请参阅*配置 NIC 设置*，第 292 页）。

15 故障排除

在联系技术支持之前，请使用此部分查找常见问题的解决方案。

Websense 网站设有一个内容广泛的知识库，网址为 www.websense.com/global/en/SupportAndKB/。您可按照关键字或参考编号搜索主题，也可浏览最热门文章。

故障排除说明被分类归入以下部分：

安装和订购问题

Websense 状态会显示订购问题

下载 Websense 主数据库和执行 Internet 筛选必须提供有效的订购密钥。当您的订购过期或无效，以及超过 2 周尚未下载主数据库时，Websense 运行状况监视器将显示警告信息。

- 请检查您是否已正确输入所收到的订购密钥。密钥区分大小写。
- 请确保您的订购尚未过期。请参阅 *订购密钥*，第 300 页。

- 请确保在最近 2 周内成功下载了主数据库。您可以在 Websense Manager 中查看下载状态：单击 “状态” > “今天” 页面上的**数据库下载**。

  请参阅*主数据库未下载*，第 299 页，以获取对数据库下载问题进行故障排除的帮助。

如果您已正确输入了密钥，但继续收到状态错误消息，或者您的订购已过期，请联系 Websense, Inc. 或您的授权经销商。

当您的订购过期时， Websense Manager 设置将决定是为所有用户授予未筛选的 Internet 访问权限还是阻止所有 Internet 请求。请参阅*您的订购*，第 25 页，以了解更多信息。

升级之后， Websense Manager 中的用户将会丢失

如果您已将 Active Directory 定义为您的目录服务，则 Websense 软件升级之后，用户名可能不会显示在 Websense Manager 中。当用户名中包含不属于 UTF-8 字符集的字符时会出现这种情况。

为了支持 LDAP 3.0， Websense 安装程序在升级期间将字符集从 MBCS 更改为 UTF-8。因此，包含非 UTF-8 字符的用户名将无法被正确识别。

要解决此问题，请手动将字符集更改为 MBCS：

1. 在 Websense Manager 中，转至**设置** > **目录服务**。
2. 请确保在页面顶部附近的 “目录” 下选中 **Active Directory (Native Mode)**。
3. 单击**高级目录设置**。
4. 在 “字符集” 下，单击 **MBCS**。您可能需要向下滚动才能看到此选项。
5. 单击**确定**以缓存更改。直到您单击**全部保存**之后，更改才会生效实施。

主数据库问题

初始筛选数据库正在使用中

Websense 主数据库可存储为筛选 Internet 内容提供基础的类别和协议定义。

部分版本的主数据库与您的 Websense 软件一起安装在每台 Filtering Service 计算机上。这个部分数据库将用于从您输入订购密钥开始即启用基本的筛选功能。

必须下载完整的数据库才能实现完全筛选。请参阅 *Websense 主数据库*，第 28 页，以了解更多信息。

下载完整数据库可能需要数分钟时间，甚至可能超过 60 分钟，这取决于互联网连接速度、带宽、可用内存和空余磁盘空间等因素。

主数据库是一周以前的

Websense 主数据库可存储为筛选 Internet 内容提供基础的类别和协议定义。Websense 软件会根据 Websense Manager 中定义的计划将更改下载到主数据库。默认情况下，下载按计划每天进行一次。

要手动启动数据库下载：

1. 在 Websense Manager 中，转至**状态 > 今天**页面，然后单击**数据库下载**。
2. 单击相应 Filtering Service 实例旁边的**更新**启动数据库下载，或单击**全部更新**在所有 Filtering Service 计算机上启动下载。

   注意

   在将更新下载到主数据库后，将数据库载入本地内存时 CPU 使用率会暂时达到 90% 或更高。建议在非高峰时段进行下载。

3. 要在下载数据库的同时继续工作，请单击**关闭**。

   在任意时间单击**数据库下载**按钮可查看下载状态。

如果主数据库的新版本中添加或删除了类别或协议，则在下载时执行与类别或协议有关的策略管理任务（如编辑类别集）的管理员可能会收到错误。虽然这类更新并不常见，但作为最佳实践，请尽量避免在进行数据库更新时进行与类别和协议有关的更改。

主数据库未下载

如果您无法成功地下载 Websense 主数据库：

- 请确保您已经在 Websense Manager 中正确输入了订购密钥，且密钥尚未过期（*订购密钥*，第 300 页）。
- 请验证 Filtering Service 计算机是否能够访问 Internet（*Internet 访问*，第 300 页）。
- 请检查防火墙或代理服务器设置，确保 Filtering Service 可以连接到 Websense 下载服务器（*验证防火墙或代理服务器设置*，第 301 页）。
- 请确保下载计算机上有足够的磁盘空间（*磁盘空间不足*，第 301 页）和内存（*内存不足*，第 302 页）。
- 请查找网络中可能阻止下载连接的任何应用程序或设备，例如防病毒软件（*限制应用程序*，第 303 页）。

订购密钥

要验证订购密钥输入正确无误且尚未过期：

1. 在 Websense Manager 中，转至**设置 > 帐户**。
2. 将从 Websense, Inc. 或经销商处获得的密钥与**订购密钥**字段进行比较。密钥使用的大小写必须与密钥文档中的大小写相同。
3. 查看**密钥过期**旁边的日期。如果日期已过，请联系您的经销商或 Websense, Inc. 以续订订购。
4. 如果您在 “设置” 对话框中对密钥进行了更改，请单击**确定**激活密钥并启用数据库下载。

要手动启动数据库下载，或要查看最近数据库下载的状态，请单击 “状态” > “今天” 页面顶部工具栏中的**数据库下载**。

Internet 访问

要下载主数据库，Filtering Service 计算机会将一个 **HTTP post** 命令发送到下载服务器，其 URL 如下：

download.websense.com
ddsdom.websense.com
ddsint.websense.com
portal.websense.com
my.websense.com

要验证 Filtering Service 是否具有与下载服务器进行通讯所必需的 Internet 访问权限：

1. 在运行 Filtering Service 的计算机上打开浏览器。
2. 输入下列 URL：

   http://download.websense.com/

   如果计算机能够打开至该站点的 HTTP 连接，将显示一个重定向页面，然后浏览器会显示 Websense 主页。

   如果没有发生这些情况，请确保该计算机：

   - 能够通过端口 80 或您的网络中为 HTTP 通信指定的端口进行通讯
   - 被配置为正确地执行 DNS 查找
   - 被配置为使用任何必要的代理服务器（请参阅*验证防火墙或代理服务器设置*，第 301 页）

   此外，还请确保您的网关没有包含任何阻止来自 Filtering Service 计算机的 HTTP 通信的规则。
3. 使用下列方法之一确认计算机能够与下载站点进行通讯：
   - 在命令提示符下输入下列命令：

     ```
     ping download.websense.com
     ```

     验证 ping 是否能收到来自下载服务器的回复。
   - 使用 telnet 连接 **download.websense.com 80**。如果看到光标且没有任何错误消息，则您可以连接到下载服务器。

验证防火墙或代理服务器设置

如果主数据库通过要求进行身份验证的防火墙或代理服务器进行下载，请确保 Filtering Service 计算机上的浏览器能够正确地加载网页。如果页面正常打开，但主数据库没有下载，请检查网络浏览器中的代理服务器设置。

Microsoft Internet Explorer：

1. 选择**工具 > Internet 选项**。
2. 打开**连接**选项卡。
3. 单击 **LAN 设置**。代理服务器配置信息将显示在**代理服务器**下面。

   记下代理设置。

Mozilla Firefox：

1. 选择**工具 > 选项 > 高级**。
2. 选择**网络**选项卡。
3. 单击**设置**。“连接设置”对话框将显示浏览器是否被配置为连接到代理服务器。

   记下代理设置。

接下来，确保 Websense 软件被配置为使用相同的代理服务器执行下载。

1. 在 Websense Manager 中，转至**设置 > 数据库下载**。
2. 验证**使用代理务器或防火墙**是否已选中，以及是否列出了正确的服务器和端口。
3. 确保**身份验证**设置正确无误。验证用户名和密码，检查拼写和大小写。

   如果 Websense 软件必须提供身份验证信息，则防火墙或代理服务器必须被配置为接受明文或基本身份验证。有关启用基本身份验证的信息，请参阅 Websense 知识库。

如果防火墙在 Websense 软件正常下载数据库时限制 Internet 访问，或限制可通过 HTTP 传输的文件大小，则 Websense 软件将无法下载数据库。要确定是否防火墙导致了下载失败，请在防火墙上搜索可能阻止下载的规则，并在必要时更改 Websense Manager 中的下载时间 （*配置数据库下载*，第 30 页）。

磁盘空间不足

Websense Master Database 存储在 Websense **bin** 目录 （默认情况下为 /opt/Websense/bin 或 C:\Program Files\Websense\bin）中。包含此目录的驱动器必须具有足以下载压缩数据库的空间，且有足够的空间解压缩数据库。

计算机的可用磁盘空间至少要达到主数据库大小的 2 倍。随着主数据库中项的增加，成功下载所需的磁盘空间大小也会增加。作为一般规则，Websense, Inc. 建议下载驱动器上至少要有 3 GB 的可用磁盘空间。

在 Windows 中，请使用 Windows 资源管理器来检查可用磁盘空间：

1. 在 Windows 资源管理器 （不是 Internet Explorer）中打开**我的电脑**。
2. 选择安装 Websense 软件的驱动器。默认情况下，Websense 软件位于 C 驱动器上。
3. 右键单击并从弹出菜单中选择**属性**。
4. 在 “常规” 选项卡上，验证是否拥有至少 3 GB 的可用空间。如果驱动器上的可用空间不足，请删除不必要的文件以释放所需空间。

在 Linux 系统中，请使用 **df** 命令来验证安装 Websense 软件的文件系统中的可用空间大小：

1. 打开终端会话。
2. 在提示符下输入：

   ```
   df -h /opt
   ```

   Websense 软件通常安装在 /opt/Websense/bin 目录中。如果安装在其他位置，请使用相应路径。
3. 确保至少拥有 3 GB 可用空间。如果驱动器上的可用空间不足，请删除不必要的文件以释放所需空间。

如果您证实有足够的磁盘空间，但仍然存在下载问题，请尝试停止所有 Websense 服务 （请参阅 *停止和启动 Websense 服务*，第 238 页），删除 **Websense.xfr** 和 **Websense** （无扩展名）文件，启动服务，然后手动下载新数据库。

内存不足

运行 Websense 软件和下载主数据库所需的内存有所不同，具体取决于网络的大小。例如，在小型网络中，建议所有平台都使用 2 GB 内存。

请参阅 *部署指南* 了解系统建议。

在 Windows 系统中检查内存：

1. 打开 “任务管理器”。
2. 选择**性能**选项卡。
3. 查看可用**物理内存**总数。
4. 如果安装的物理内存小于 2 GB，请升级计算机中的 RAM。

也可以选择**控制面板 > 管理工具 > 性能**来获取信息。

在 Linux 系统中检查内存：

1. 打开终端会话。
2. 在提示符下输入：

   ```
   top
   ```
3. 通过添加 **Mem: av** 和 **Swap: av** 计算可用内存总数。
4. 如果安装的物理内存小于 2 GB，请升级计算机中的 RAM。

限制应用程序

某些限制应用程序或设备 （例如病毒扫描器、限制大小的应用程序或入侵检测系统）可能会影响数据库下载。理想情况下，应将 Websense 软件配置为直接到达最后一个网关，以便它不会连接到这些应用程序或设备。也可以：

1. 禁用与 Filtering Service 计算机和主数据库下载位置有关的限制。

   请参阅设备或软件文档，以了解有关更改设备配置的说明。
2. 尝试下载主数据库。

如果更改不起作用，请将应用程序或设备重新配置为包括运行 Filtering Service 的计算机。

主数据库下载没有在正确的时间进行

Filtering Service 计算机上的系统日期和时间可能没有正确设置。 Websense 软件使用系统时钟来确定下载主数据库的正确时间。

如果根本没有进行下载，请参阅*主数据库未下载*，第 299 页。

就数据库下载问题联系技术支持

如果在完成本帮助部分中的故障排除步骤之后，仍然遇到主数据库下载问题，请将下列信息发送至 Websense 技术支持：

1. 在 “数据库下载”对话框中出现的确切错误消息
2. 尝试下载数据库的计算机的外部 IP 地址
3. 您的 Websense 订购密钥
4. 最后一次尝试的日期和时间
5. 传送的字节数 （如果有）
6. 打开命令提示符并对 **download.websense.com** 执行 **nslookup**。如果进行了与下载服务器的连接，请将返回的 IP 地址发送给技术支持。
7. 打开命令提示符并对 **download.websense.com** 执行 **tracert**。如果进行了与下载服务器的连接，请将路由追踪发送给技术支持。
8. 尝试下载期间在 Websense 下载服务器上执行的数据包追踪或数据包捕获。
9. 同一次尝试下载期间在网络网关上执行的数据包追踪或数据包捕获。
10. Websense **bin** 目录中的下列文件：**websense.ini**、**eimserver.ini** 和 **config.xml**。

请转至 www.websense.com/SupportPortal/default.aspx 获取技术支持联系信息。

筛选问题

Filtering Service 未在运行

当 Filtering Service 未运行时， Internet 请求无法被筛选和记录。

在下列情况下， Filtering Service 可能会停止运行：

- Filtering Service 计算机上的磁盘空间不足。
- 主数据库下载由于磁盘空间不足而失败 （请参阅*主数据库未下载*，第 299 页）。
- **websense.ini** 文件丢失或损坏。
- 您停止了服务 （例如在创建自定义阻止页面后）且没有重新启动它。

如果您重新启动了多个 Websense 服务而它们未按照正确的顺序启动，则 Filtering Service 也可能会停止。在重新启动多项服务时，请切记要首先启动 Policy Database、Policy Broker 和 Policy Server，然后再启动其他 Websense 服务。

要对这些问题进行故障排除：

- 确保在 Filtering Service 计算机上至少有 3 GB 可用磁盘空间。您可能需要删除不使用的文件或增加额外容量。
- 转至 Websense **bin** 目录 （默认情况下为 C:\Program Files\Websense\bin 或 /opt/Websense/bin），确认您可以在文本编辑器中打开 **websense.ini**。如果此文件已被损坏，请用备份文件将其替换。
- 检查 Windows 事件查看器或 **websense.log** 文件以查看来自 Filtering Service 的错误消息 （请参阅*故障排除工具*，第 334 页）。
- 注销 Websense Manager，重新启动 Websense Policy Server，然后重新启动 Websense Filtering Service（请参阅*停止和启动 Websense 服务*，第 238 页）。

  等待 1 分钟，然后再次登录 Websense Manager。

User Service 不可用

如果 User Service 没有运行或 Policy Server 无法与 User Service 进行通讯，则 Websense 软件无法正确地应用基于用户的筛选策略。

如果您是在重新启动其他 Websense 服务之后才重新启动 Policy Server，则 User Service 可能会停止。要纠正此问题：

1. 重新启动 Websense Policy Server 服务（请参阅*停止和启动 Websense 服务*，第 238 页）。
2. 启动或重新启动 Websense User Service。
3. 关闭 Websense Manager。

   等待 1 分钟，然后再次登录 Websense Manager。

如果前面的步骤没有解决该问题：

- 检查 Windows 事件查看器或 **websense.log** 文件以查看来自 User Service 的错误消息（请参阅*故障排除工具*，第 334 页）。
- 转至 Websense **bin** 目录（默认情况下为 C:\Program Files\Websense\bin 或 /opt/websense/bin），确保您可以在文本编辑器中打开 **websense.ini**。如果此文件已被损坏，请用备份文件将其替换。

站点被不正确地分类为信息技术

Internet Explorer 4.0 或更高版本可以接受从地址栏进行搜索。在启用此选项时，如果用户仅在地址栏中输入了域名（例如 **websense** 而不是 **http://www.websense.com**），则 Internet Explorer 会将输入视为搜索请求而不是站点请求。它会同时显示用户最可能搜索的站点以及近似匹配站点的列表。

因此，Websense 软件会根据活动策略中的信息技术/搜索引擎和门户类别的状态 — 而不是所请求站点的类别来允许、阻止或限制请求。要想让 Websense 软件根据所请求站点的类别进行筛选，您必须关闭从地址栏中搜索：

1. 转至**工具 > Internet 选项**。
2. 转至**高级**选项卡。
3. 在“从地址栏中搜索”下面，选择**不从地址栏中搜索**。
4. 单击**确定**。

> **注意**
> 这些步骤适用于 Internet Explorer 5、 6 和 7。

关键字未被阻止

造成此问题的可能原因有 2 种：**禁用关键字阻止**被选中，或 URL 中包含关键字的站点使用 **post** 向您的 Web 服务器发送数据。

要确保已启用关键字阻止：

1. 在 Websense Manager 中，转至**设置 > 筛选**。
2. 在“常规筛选”下，查看**关键字搜索选项**列表。如果显示了**禁用关键字阻止**，请选择列表中的另一个选项。请参阅*配置 Websense 筛选设置*，第 49 页，以了解有关可用选项的更多信息。
3. 单击**确定**以缓存更改。直到您单击**全部保存**之后，更改才会生效实施。

如果站点使用 **post** 向 Web 服务器发送数据，则 Websense 软件不会识别该 URL 的关键字筛选设置。除非您的集成产品可识别通过 post 发送的数据，否则用户仍然能够访问包含被阻止关键字的 URL。

要查看某个站点是否使用 post 命令，请从您的浏览器中查看站点源。如果源代码包含类似于 **<method=post>** 的字符串，则 post 被用于加载该站点。

自定义或受限访问筛选器 URL 没有按照预期进行筛选

如果受限访问筛选器或自定义 URL 列表（重新分类或未筛选）中的 HTTPS URL 未按照预期进行筛选，则集成产品可能将 URL 转换为了 Filtering Service 无法识别的格式。

非代理集成产品会将 URL 从域格式转换为 IP 格式。例如，URL **https://<domain>** 被读为 **https://<IP 地址>:443**。出现这种情况时，Filtering Service 无法将从集成产品接收的 URL 与自定义 URL 或受限访问筛选器进行匹配，相应地也不会筛选该站点。

要解决此问题，请同时添加要使用自定义 URL 或受限访问筛选器进行筛选的站点的 IP 地址和 URL。

用户无法按照预期访问协议或应用程序

如果您的网络包含 Microsoft ISA Server，则某些身份验证方法配置可能会导致与消息应用程序的连接中断。

如果启用了匿名身份验证之外的任何方法，则代理服务器会在用户请求应用程序连接时尝试识别所接收的数据包。由于代理服务器无法识别数据包，因此连接中断。这可能会导致 Websense 协议筛选活动出现偏差。

如果应用程序使用的端口被阻止，也可能会出现无法访问协议或 Internet 应用程序的情况。可能导致这种情况的原因包括：

- 端口被防火墙阻止。
- 被阻止的自定义协议在其任意标识符中包含该端口（作为单个端口或端口范围的一部分）。

FTP 请求未按照预期被阻止

在与 Check Point® 防火墙相集成时， Websense 软件需要在客户端的浏览器中启用**文件夹视图**以识别和筛选 FTP 请求。

在未启用文件夹视图时，发送到 FireWall-1 代理的 FTP 请求会被以“http://”为前缀发送到 Websense 软件。因此，Websense 软件会将这些请求视为 HTTP 请求而非 FTP 请求来进行筛选。

Websense 软件没有应用用户策略或组策略

如果 Websense 软件正在应用计算机或网络策略，或者**默认**策略（即使在分配了用户策略或组策略之后），请参阅*用户标识问题*，第 309 页。其他信息请参阅知识库。

远程用户没有按正确的策略进行筛选

如果远程用户通过使用缓存的域凭据 （网络登录信息）登录来访问网络，则 Websense 软件会应用分配到该用户，或分配到该用户的组或域的策略 （如果适用）。如果没有任何策略被分配到用户、组或域，或者用户使用本地用户帐户登录到计算机，则 Websense 软件会应用默认策略。

有时，用户未按用户或组策略、或默认策略进行筛选。如果用户使用本地用户帐户登录远程计算机，且远程计算机媒体访问控制 (MAC) 地址的最后部分与已分配策略的网络内 IP 地址重叠，则会出现这种情况。在这种情况下，分配到该特定 IP 地址的策略将被应用于远程用户。

Network Agent 问题

- *没有安装 Network Agent*，第 307 页
- *Network Agent 未在运行*，第 308 页
- *Network Agent 没有监视任何 NIC*，第 308 页
- *Network Agent 无法与 Filtering Service 进行通讯*，第 308 页

没有安装 Network Agent

Network Agent 是启用协议筛选所必需的。通过使用某些集成产品，Network Agent 还可用于提供更精确的日志记录。

如果您正在运行集成产品，且不需要 Network Agent 协议筛选或日志记录，您可以隐藏 “没有安装 Network Agent” 状态消息。请参阅*查看当前系统状态*，第 245 页，以了解相关说明。

对于独立安装，必须安装 Network Agent 才能监视和筛选网络通信。请参阅*安装指南*以了解相关安装说明，然后参阅*Network Agent 配置*，第 289 页。

Network Agent 未在运行

Network Agent 是启用协议筛选所必需的。通过使用某些集成产品， Network Agent 还可用于提供更精确的日志记录。

对于独立安装，必须运行 Network Agent 才能监视和筛选网络通信。

要对此问题进行故障排除：

1. 查看 “Windows 服务”对话框 （请参阅 *Windows 服务对话框*，第 334 页）以了解是否启动了 **Websense Network Agent** 服务。
2. 重新启动 **Websense Policy Broker** 和 **Websense Policy Server** 服务 （请参阅 *停止和启动 Websense 服务*，第 238 页）。
3. 启动或重新启动 **Websense Network Agent** 服务。
4. 关闭 Websense Manager。
5. 等待 1 分钟，然后再次登录 Websense Manager。

如果这样不能解决问题：

- 请检查 **Windows 事件查看器**以查看来自 Network Agent 的错误消息（请参阅 *Windows 事件查看器*，第 335 页）。
- 请检查 **Websense.log** 文件以查看来自 Network Agent 的错误消息 （请参阅 *Websense 日志文件*，第 335 页）。

Network Agent 没有监视任何 NIC

Network Agent 必须被关联到至少一个网络接口卡 (NIC) 才能监视网络通信。

如果您在 Network Agent 计算机上添加或移除了网卡，则必须更新您的 Network Agent 配置。

1. 在 Websense Manager 中，转至**设置**。
2. 在左侧导航窗格的 Network Agent 下，选择 Network Agent 计算机的 IP 地址。
3. 验证是否选定计算机的所有 NIC 均被列出。
4. 验证是否至少有一个 NIC 被设置为监视网络通信。

请参阅 *Network Agent 配置*，第 289 页，以了解更多信息。

Network Agent 无法与 Filtering Service 进行通讯

Network Agent 必须能够使用 Filtering Service 通讯，以强制执行您的 Internet 使用策略。

- 您是否更改了 Filtering Service 计算机的 IP 地址或重新安装了 Filtering Service?
  如果是，请参阅 *更新 Filtering Service IP 地址或 UID 信息*，第 309 页。
- 您的 Network Agent 计算机上是否有 2 个以上网络接口卡 (NIC)?
  如果是，请参阅 *网络配置*，第 287 页，以验证您的 Websense 软件设置。

- 您是否重新配置了连接到 Network Agent 的交换机？

  如果是，请参阅*安装指南*以验证您的硬件设置，并参阅 *Network Agent 配置*，第 289 页，以验证您的 Websense 设置。

如果这些都不适用，请参阅*配置本地设置*，第 291 页，以了解有关将 Network Agent 和 Filtering Service 相关联的信息。

更新 Filtering Service IP 地址或 UID 信息

在卸载和重新安装 Filtering Service 时， Network Agent 不会自动更新 Filtering Service 的内部标识符 (UID)。 Websense Manager 会尝试使用已不存在的旧 UID 向 Filtering Service 进行查询。

与之类似，当您更改 Filtering Service 计算机的 IP 地址时，此更改也不会自动注册。

要重新建立与 Filtering Service 的连接：

1. 打开 Websense Manager。

   将出现一条状态消息，表示 Network Agent 实例无法连接到 Filtering Service。
2. 单击左侧导航窗格顶部的**设置**。
3. 在左侧导航窗格的 Network Agent 下，选择 Network Agent 计算机的 IP 地址。
4. 在页面顶部的“Filtering Service 定义”下面，展开**服务器 IP 地址**列表，然后选择 Filtering Service 计算机的 IP 地址。
5. 单击页面底部的**确定**以缓存更新。直到您单击**全部保存**之后，更改才会生效实施。

用户标识问题

相关主题：

- *筛选问题*，第 304 页
- *未提示远程用户进行手动身份验证*，第 318 页
- *远程用户未被正确地筛选*，第 318 页

如果 Websense 软件正在使用计算机或网络策略、或者**默认**策略来筛选 Internet 请求（即使是在您已经分配了基于用户或组的策略之后），或者正在应用错误的基于用户或组的策略，请使用下列步骤来查明问题：

- 如果您正在使用 Microsoft ISA Server 且更改了其身份验证方法，请确保重新启动 Web Proxy Service。

- 如果您正在使用 Windows Active Directory 中的嵌套组，则分配到父组的策略会被应用于属于子组的用户，而不是直接应用于父组。有关用户和组层级结构的信息，请参阅您的目录服务文档。
- User Service 缓存可能已过期。User Service 缓存用户名与 IP 地址映射的时间为 3 个小时。您可以通过缓存 Websense Manager 中的所有更改，然后单击**全部保存**来强制更新 User Service 缓存。
- 如果用户是在运行 Windows XP SP2 的计算机上被不正确地筛选，则问题可能是由于 Windows Internet 连接防火墙 (ICF)（包括在 Windows XP SP2 中且默认情况下处于启用状态）所造成的。有关 Windows ICF 的更多信息，请参阅 Microsoft 知识库文章 #320855。

  DC Agent 或 Logon Agent 从运行 Windows XP SP2 的计算机获取用户登录信息的步骤：

  1. 从客户端计算机的 Windows **开始**菜单中，选择**设置** > **控制面板** > **安全中心** > **Windows 防火墙**。
  2. 转至**例外**选项卡。
  3. 选中**文件和打印机共享**。
  4. 单击**确定**关闭 ICF 对话框，然后关闭所有其他打开的窗口。

如果您正在使用 Websense 透明标识代理，请参阅相应的故障排除部分：

- *DC Agent 故障排除*，第 310 页。
- *Logon Agent 故障排除*，第 312 页。
- *eDirectory Agent 故障排除*，第 314 页。
- *RADIUS Agent 故障排除*，第 316 页。

DC Agent 故障排除

要对 DC Agent 的用户标识问题进行故障排除：

1. 检查所有网络连接。
2. 检查 Windows 事件查看器以查看错误消息（请参阅*Windows 事件查看器*，第 335 页）。
3. 检查 Websense 日志文件 (Websense.log) 以查看详细的错误信息 （请参阅*Websense 日志文件*，第 335 页）。

DC Agent 用户标识问题的常见原因包括：

- 网络或 Windows 服务正在与域控制器进行通讯的方式使 DC Agent 将服务视为一个尚未对其定义策略的新用户。请参阅*用户未按默认策略进行正确筛选*，第 311 页。
- DC Agent 或 User Service 可以被安装为一项使用来宾帐户（相当于域控制器的匿名用户）的服务。如果域控制器被设置为不向匿名用户提供用户和组列表，则将不允许 DC Agent 下载列表。请参阅*手动更改 DC Agent 和 User Service 权限*，第 311 页。

- User Service 缓存已过期。默认情况下，User Service 缓存用户名与 IP 地址映射的时间为 3 个小时。您每次在 Websense Manager 中进行更改并单击**全部保存**之后，该缓存也会被更新。

用户未按默认策略进行正确筛选

当某个网络或 Microsoft Windows 200x 联系域控制器时，它们使用的帐户名可能会导致 Websense 软件认为有一个未识别的用户正在从已筛选的计算机访问 Internet。由于尚未给此用户分配基于用户或组的策略，因此会应用计算机或网络策略，或者应用默认策略。

- 网络服务可能需要域权限才能访问网络上的数据，并使用它们在其下运行的域用户名联系域控制器。

  要解决此问题，请参阅*将代理配置为忽略特定的用户名*，第 196 页。

- Windows 200x 服务使用由计算机名后跟美元符号 (jdoe-computer$) 组成的用户名定期联系域控制器。DC Agent 会将该服务视为一个尚未向其分配策略的新用户。

  要解决此问题，请将 DC Agent 配置为忽略形式为 **computer$** 的所有登录。

  1. 在 DC Agent 计算机上，转至 Websense **bin** 目录 （默认情况下为 **C:\Program Files\Websense\bin**）。
  2. 在文本编辑器中打开 **transid.ini** 文件。
  3. 将下列项添加到该文件中：

     ```
     IgnoreDollarSign=true
     ```

  4. 保存并关闭文件。
  5. 重新启动 DC Agent （请参阅*停止和启动 Websense 服务*，第 238 页）。

手动更改 DC Agent 和 User Service 权限

在运行域控制器的计算机上：

1. 创建一个用户帐户，如 **Websense**。您可以使用现有帐户，但建议使用 Websense 帐户，这样可将密码设置为不过期。不需要特殊权限。

   将密码设置为永不过期。此帐户仅可为访问目录对象提供安全上下文。

   记下您为此帐户建立的用户名和密码，因为在步骤 6 和 7 中必须输入这些信息。
2. 打开每个 Websense DC Agent 计算机上的 “Windows 服务”对话框 （转至 **开始 > 程序 > 管理工具 > 服务**）。
3. 选择 **Websense DC Agent** 项，然后单击**停止**。
4. 双击 **Websense DC Agent** 项。
5. 在**登录**选项卡上，选中**此帐户**选项。
6. 输入在步骤 1 中创建的 Websense DC Agent 帐户的用户名。例如：**DomainName\websense**。

7. 输入此帐户的 Windows 密码并确认。
8. 单击**确定**关闭对话框。
9. 在 “服务”对话框中选择 **Websense DC Agent** 项，然后单击**启动**。
10. 对 Websense User Service 的每个实例重复此过程。

Logon Agent 故障排除

如果您的网络中的某些用户由于 Logon Agent 未能识别它们而被**默认**策略筛选：

- 请确保 Windows 组策略对象 (GPO) 被正确地应用于这些用户的计算机（请参阅*组策略对象*，第 312 页）。
- 如果 User Service 安装在 Linux 计算机上且您正在使用 Windows Active Directory (Native Mode)，请检查您的目录服务配置（请参阅*在 Linux 上运行的 User Service*，第 313 页）。
- 请验证客户端计算机是否能够与运行登录脚本的域控制器进行通讯（请参阅*域控制器可见性*，第 313 页）。
- 请确保在客户端计算机上启用了 NetBIOS （请参阅*NetBIOS*，第 313 页）。
- 请确保客户端计算机上的用户配置文件没有损坏 （请参阅*用户配置文件问题*，第 314 页）。

组策略对象

在验证您的环境满足 Websense 软件*安装指南*中描述的先决条件之后，确保组策略对象被正确地应用：

1. 在 Active Directory 计算机上，打开 Windows 控制面板并转至**管理工具 > Active Directory 用户和计算机**。
2. 右键单击域项，然后选择**属性**。
3. 单击**组策略**选项卡，然后从 “组域策略对象链接”列表中选择域策略。
4. 单击**编辑**，然后在目录树中展开用户配置节点。
5. 展开 Windows 设置节点，然后选择**脚本**。
6. 在右侧窗格中，双击**登录**，然后验证 **logon.bat** 是否在 “登录属性”对话框中列出。

   此脚本是客户端登录应用程序所必需的。

   - 如果 **logon.bat** 没有在脚本中，请参阅 Websense 软件*安装指南*中的*初始设置*一章。
   - 如果 **logon.bat** 出现在脚本中，但 Logon Agent 没有运行，请使用本部分中的其他故障排除步骤来验证是否存在网络连接问题，或参阅 Websense 知识库。

在 Linux 上运行的 User Service

当您将 Logon Agent 用于用户的透明标识，且 User Service 安装在 Linux 计算机上时，您必须暂时将 Websense 配置为与 Active Directory (Mixed Mode) 进行通讯。

1. 在 Websense Manager 中，转至**设置 > 目录服务**。
2. 记下您当前的目录设置。
3. 在“目录”下，选择 **Windows NT Directory / Active Directory (Mixed Mode)**。
4. 单击**确定**以缓存更改，然后单击**全部保存**。
5. 在“目录”下，选择 **Active Directory (Native Mode)**。如果您的原始配置没有出现，请使用在步骤 2 中记录的笔记重新创建目录设置。请参阅 *Windows Active Directory (Native Mode)*，第 55 页，以了解详细说明。
6. 完成配置更改之后，单击**确定**，然后单击**全部保存**。

域控制器可见性

要验证客户端计算机是否能够与域控制器进行通讯：

1. 尝试将客户端计算机上的驱动器映射到域控制器的根共享驱动器。这是通常情况下登录脚本运行的位置， **LogonApp.exe** 就位于此处。
2. 在客户端计算机上，打开 Windows 命令提示符，然后执行下列命令：

   ```
   net view /domain:<domain name>
   ```

如果这些测试失败，请参阅 Windows 操作系统文档以获取可能的解决方案。存在与 Websense 软件无关的网络连接问题。

NetBIOS

必须对 TCP/IP 启用 NetBIOS 且 TCP/IP NetBIOS Helper 服务必须运行，Websense 登录脚本才能在用户的计算机上运行。

要确保在客户端计算机上为 TCP/IP 启用 NetBIOS：

1. 右键单击**网上邻居**，然后选择**属性**。
2. 右键单击**本地连接**，然后选择**属性**。
3. 选择 **Internet 协议 (TCP/IP)**，然后单击**属性**。
4. 单击**高级**。
5. 选择 **WINS** 选项卡，然后验证是否设置了正确的 NetBIOS 选项。
6. 如果进行了更改，请单击**确定**，然后再两次单击**确定**关闭其他“属性”对话框并保存更改。

   如果不需要进行更改，请单击**取消**关闭每个对话框而不进行更改。

使用“Windows 服务”对话框验证客户端计算机上是否运行了 **TCP/IP NetBIOS Helper** 服务（请参阅 *Windows 服务对话框*，第 334 页）。 TCP/IP NetBIOS Helper 服务可运行于 Windows 2000、 Windows XP、 Windows Server 2003 和 Windows NT 上。

用户配置文件问题

如果客户端计算机上的用户配置文件损坏，则 Websense 登录脚本（和 Windows GPO 设置）将无法运行。此问题可通过重新创建用户配置文件解决。

当您重新创建用户配置文件时，用户的现有 My Documents 文件夹、收藏报告以及其他自定义数据和设置不会自动转移到新配置文件中。在确认新配置文件已经解决问题并将用户现有数据复制到新配置文件之前，请不要删除现有的已损坏配置文件。

要重新创建用户配置文件：

1. 以本地管理员身份登录客户端计算机。
2. 重命名包含用户配置文件的目录：

   ```
   C:\Documents and Settings\<用户名>
   ```

3. 重新启动计算机。
4. 作为已筛选的用户登录计算机。系统将自动创建新的用户配置文件。
5. 检查以确保按照预期筛选用户。
6. 将自定义数据（例如 My Documents 文件夹中的内容）从旧配置文件复制到新配置文件。请不要使用“文件和设置转移向导”，它可能会将损坏内容转移到新配置文件。

eDirectory Agent 故障排除

相关主题：

- *启用 eDirectory Agent 诊断*，第 315 页
- *eDirectory Agent 误算 eDirectory Server 连接*，第 316 页
- *以控制台模式运行 eDirectory Agent*，第 316 页

如果用户名没有传送到 eDirectory Agent，则用户不会被正确地筛选。如果用户没有登录 Novell eDirectory 服务器，则 eDirectory Agent 不能检测登录。发生这种情况的原因是：

- 用户登录的域未包括在 eDirectory 用户登录会话的默认根上下文中。此根上下文是在安装期间指定的，应当与在**设置** > **目录服务**页面上为 Novell eDirectory 指定的根上下文相匹配。
- 用户试图绕过登录提示符以避开 Websense 筛选。
- 用户没有在 eDirectory 服务器中设置帐户。

如果用户没有登录 eDirectory 服务器，则特定于用户的策略不能被应用于该用户，而是将应用**默认**策略。如果在用户匿名登录的网络中存在共享工作站，请为这些特定的计算机设置筛选策略。

要确定 eDirectory Agent 是否接收用户名和识别该用户：

1. 激活 eDirectory Agent 日志记录，如*启用 eDirectory Agent 诊断*，第 315 页所述。
2. 在文本编辑器中打开您所指定的日志文件。
3. 搜索与未被正确筛选的用户相对应的项。
4. 类似于下列情况的项表示 eDirectory Agent 已识别了用户：

   ```
   WsUserData::WsUserData()
   User: cn=Admin,o=novell (10.202.4.78)
   WsUserData::~WsUserData()
   ```

   在上面的示例中，用户 **Admin** 登录 eDirectory 服务器并被成功识别。
5. 如果用户被识别，但仍未按照预期被筛选，请检查您的策略配置以验证是否对该用户应用了合适的策略，以及 Websense Manager 中的用户名是否与 Novell eDirectory 中的用户名相对应。

   如果用户*未*被识别，请验证：

   - 该用户有 Novell eDirectory 帐户。
   - 该用户登录的域包括在 eDirectory 用户登录的默认根上下文中。
   - 该用户没有绕过登录提示符。

启用 eDirectory Agent 诊断

eDirectory Agent 具有内置诊断功能，但这些功能在默认情况下没有激活。您可以在安装期间启用日志记录和调试，也可随时启用它们。

1. 停止 eDirectory Agent （请参阅*停止和启动 Websense 服务*，第 238 页）。
2. 在 eDirectory Agent 计算机上，转至 eDirectory Agent 安装目录。
3. 在文本编辑器中打开文件 **wsedir.ini**。
4. 找到 **[eDirAgent]** 部分。
5. 要启用日志记录和调试，请将 **DebugMode** 的值更改为 **On**：

   ```
   DebugMode=On
   ```
6. 要指定日志的详细级别，请修改下列行：

   ```
   DebugLevel=<N>
   ```

   N 可以是 0-3 之间的值，其中 3 表示最详细。
7. 修改 **LogFile** 行以指定日志输出文件的名称：

   ```
   LogFile=filename.txt
   ```

   默认情况下，日志输出被发送到 eDirectory Agent 控制台。如果您是以控制台模式运行代理（请参阅*以控制台模式运行 eDirectory Agent*，第 316 页），您可以保留默认值。
8. 保存并关闭 **wsedir.ini**文件。
9. 启动 eDirectory Agent 服务（请参阅*停止和启动 Websense 服务*，第 238 页）。

eDirectory Agent 误算 eDirectory Server 连接

如果 eDirectory Agent 在您的网络中监视的用户超过 1000 个，但仅显示 1000 个与 Novell eDirectory 服务器的连接，可能是由于 Windows API 的限制，它负责将来自 eDirectory 服务器的信息传送到 Websense eDirectory Agent。这种情况非常少见。

要解决此限制，请向 **wsedir.ini** 文件添加一个参数，它会正确地计算服务器连接（仅限 Windows）：

1. 停止 Websense eDirectory Agent 服务（请参阅*停止和启动 Websense 服务*，第 238 页）。
2. 转至 Websense **bin** 目录 （默认情况下为 **C:\Program Files\Websense\bin**）。
3. 在文本编辑器中打开 **wsedir.ini** 文件。
4. 插入一个空行，然后输入：

   ```
   MaxConnNumber = <NNNN>
   ```

   此处的 <*NNNN*> 是与 Novell eDirectory 服务器之间可能出现的最大连接数。例如，如果您的网络有 1,950 个用户，您可以输入 2000 作为最大数。
5. 保存文件。
6. 重新启动 eDirectory Agent。

以控制台模式运行 eDirectory Agent

1. 执行下列操作之一：
   - 在 Windows 命令提示符 （**开始 > 运行 > cmd**）下，输入命令：

     ```
     eDirectoryAgent.exe -c
     ```
   - 在 Linux shell 命令提示符中输入命令：

     ```
     eDirectoryAgent -c
     ```
2. 当准备停止代理时，请按 **Enter 键**。可能需要几秒钟的时间，代理才会停止运行。

RADIUS Agent 故障排除

RADIUS Agent 具有内置诊断功能，但这些功能在默认情况下没有激活。要激活 RADIUS Agent 记录和调试：

1. 停止 RADIUS Agent 服务（请参阅*停止和启动 Websense 服务*，第 238 页）。
2. 在 RADIUS Agent 计算机上，转至代理的安装目录 （默认情况下为 **Websense\bin**）。
3. 在文本编辑器中打开 **wsradius.ini** 文件。
4. 找到 **[RADIUSAgent]** 部分。
5. 要启用日志记录和调试，请将 **DebugMode** 的值更改为 **On**：

   ```
   DebugMode=On
   ```

6. 要指定日志的详细级别，请修改下列行：

   ```
   DebugLevel=<N>
   ```

   N 可以是 0-3 之间的值，其中 3 表示最详细。

7. 修改 **LogFile** 行以指明输出文件的名称：

   ```
   LogFile=filename.txt
   ```

   默认情况下，日志输出被发送到 RADIUS Agent 控制台。如果您是以控制台模式运行代理 （请参阅 *以控制台模式运行 RADIUS Agent*，第 317 页），您可以选择保留默认值。

8. 保存并关闭 **wsradius.ini** 文件。

9. 启动 RADIUS Agent 服务（请参阅 *停止和启动 Websense 服务*，第 238 页）。

如果远程用户没有按照预期被识别和筛选，可能的原因是 RADIUS Agent 和 RADIUS 服务器之间存在通讯问题。请检查 RADIUS Agent 日志中的错误以确定原因。

以控制台模式运行 RADIUS Agent

要以控制台模式 （作为应用程序）启动 RADIUS Agent，请输入下列内容：

- 在 Windows 命令提示符下：

  ```
  RadiusAgent.exe -c
  ```

- 在 Linux shell 提示符下：

  ```
  ./RadiusAgent -c
  ```

要停止代理时，请再次按 **Enter 键**。可能需要几秒钟的时间，代理才会停止运行。

RADIUS Agent 接受下列命令行参数：

注意

在 Linux 中， Websense, Inc. 建议使用所提供的脚本启动或停止 Websense RADIUS Agent (**WsRADIUSAgent start|stop**)，而不要使用 -r 和 -s 参数。

参数	描述
-i	安装 RADIUS Agent 服务/后台程序。
-r	运行 RADIUS Agent 服务/后台程序。
-s	停止 RADIUS Agent 服务/后台程序。
-c	作为应用程序进程而不是作为服务或后台程序运行 RADIUS Agent。在采用控制台模式时，RADIUS Agent 可被配置为将日志输出发送到控制台或发送到文本文件。

参数	描述
-v	显示 RADIUS Agent 的版本号。
-? -h - 帮助 <*无选项*>	在命令行上显示使用信息。列出和描述所有可能的命令行参数。

未提示远程用户进行手动身份验证

如果您已将远程用户配置为在访问 Internet 时进行手动身份验证，偶尔可能会出现单个用户未被提示进行身份验证的情况。在某些网络内 IP 地址被配置为绕过手动身份验证时，可能会发生这种情况。

当远程用户访问网络时，Websense 软件会读取计算机的媒体访问控制 (MAC) 地址的最后部分。如果这与已配置为绕过手动身份验证的网络内 IP 地址相匹配，则远程用户在访问 Internet 时将不会被提示进行手动身份验证。

一种解决方案是将网络内 IP 地址重新配置为使用手动身份验证。另一种解决方案是对受影响的远程用户禁用手动身份验证要求。

远程用户未被正确地筛选

如果远程用户未被筛选，或未按照被分配给他们的特定策略进行筛选，请检查 RADIUS Agent 日志以查看从服务器的消息 **Error receiving from server: 10060** (Windows) 或 **Error receiving from server: 0** (Linux)。

在 RADIUS 服务器没有将 RADIUS Agent 识别为客户端（RADIUS 请求的来源）时，通常会发生这种情况。请确保正确配置了 RADIUS 服务器 （请参阅*配置 RADIUS 环境*，第 184 页）。

您可以使用 RADIUS Agent 的内置诊断工具对筛选问题进行故障排除 （请参阅*RADIUS Agent 故障排除*，第 316 页）。

如果您执行了 Remote Filtering 功能 （请参阅*Filter Remote 客户端*，第 133 页），则在 Remote Filtering Client 无法与网络内的 Remote Filtering Server 进行通讯时，远程用户不能被筛选。

有关设置 Remote Filtering 的说明，请参阅 *Remote Filtering* 技术论文。

阻止消息问题

没有为被阻止的文件类型显示阻止页面

在使用文件类型阻止时，用户可能并非总会看到阻止消息。例如，当可下载文件包含在被允许站点上的内部框架 (IFRAME) 中时，发送到该框架的阻止消息会由于框架大小为零而不可见。

这只是一个显示问题，用户并不能访问或下载被阻止的文件。

用户收到浏览器错误而不是阻止页面

如果用户收到错误消息而不是阻止页面，最可能的两个原因是：

- 用户的浏览器被配置为使用外部代理。在大多数浏览器中，都有一个允许使用外部代理的设置。请确保浏览器没有被设置为使用外部代理。
- 存在识别 Filtering Service 计算机或与之进行通讯的问题。

如果用户的浏览器设置正确无误，请确保 **eimserver.ini** 文件中正确地列出了 Filtering Service 的 IP 地址。

1. 停止 **Websense Filtering Service** （请参阅*停止和启动 Websense 服务*，第 238 页）。
2. 转至 Websense **bin** 目录（默认情况下为 C:\Program Files\Websense\bin 或 /opt/Websense/bin）。
3. 在文本编辑器中打开 **eimserver.ini** 文件。
4. 在 [WebsenseServer] 下添加一个空行，然后输入下列内容：

   ```
   BlockMsgServerName = <Filtering Service IP 地址>
   ```

   例如，如果 Filtering Service IP 地址为 10.201.72.15，则输入：

   ```
   BlockMsgServerName = 10.201.72.15
   ```

5. 保存并关闭文件。
6. 重新启动 Filtering Service。

如果 Filtering Service 计算机有多个 NIC，且在编辑 **eimserver.ini** 文件后仍未正确显示阻止页面，请在 **BlockMsgServerName** 参数中尝试其他 NIC 的 IP 地址。

如果仍未显示阻止页面，请确保该用户拥有读取 Websense 阻止页面目录中文件的权限：

- Websense\BlockPages\en\Default
- Websense\BlockPages\en\Custom

如果阻止页面问题依然存在，请参阅 Websense 知识库以了解其他故障排除提示。

显示空白页面而不是阻止页面

当广告被阻止或浏览器没有正确地检测与阻止页面关联的编码时，用户可能会收到空白页面而不是阻止页面。产生这种行为的原因如下：

- 当广告类别被阻止时，Websense 软件有时会将对图形文件的请求视为广告请求，并因此显示空白图像而不是阻止消息（阻止广告的常规方法）。如果请求的 URL 以 .gif 或类似格式结束，则让用户重新输入 URL，但不要包含 *.gif 部分。
- 某些旧版本的浏览器可能不会检测阻止页面的编码。要启用正确的字符检测，请将您的浏览器配置为显示合适的字符集（UTF-8 适用于法语、德语、意大利语、西班牙语、巴西葡萄牙语、简体中文、繁体中文或朝鲜语；Shift_JIS 适用于日语）。请参阅您的浏览器文档以获取有关说明，或将浏览器升级到较新版本。

没有按照预期显示协议阻止消息

由于存在下列原因，协议阻止消息不显示或只在延迟后显示：

- User Service 必须安装在 Windows 计算机上才能正确显示协议阻止消息。更多信息，请参阅*安装指南*。
- 如果 Network Agent 安装在具有多个网络接口卡 (NIC) 的计算机上，且 NIC 正在从 Filtering Service 监视其他网段，则协议阻止消息不会到达客户端计算机。请确保 Filtering Service 计算机具有客户端计算机的 NetBIOS 和 Server Message Block 协议访问权限且端口 15871 未被阻止。
- 当 Network Agent 被配置为监视**发送**到内部计算机的请求时，协议阻止消息会有轻微延迟，或出现在产生被请求协议数据的内部计算机上（而不是客户端计算机）。
- 如果被筛选的客户端或 Websense 筛选计算机正在运行 Windows 200x，则必须运行 Windows **Messenger** 服务才会显示协议阻止消息。使用客户端或服务器计算机上的“Windows 服务”对话框可查看 Messenger 服务是否运行（请参阅 *Windows 服务对话框*，第 334 页）。即使阻止消息没有出现，协议请求仍会被阻止。

显示协议阻止消息而不是阻止页面

如果您的集成产品没有向 Websense 软件发送 HTTPS 信息，或者 Websense 软件以独立模式运行，则 Network Agent 可能会将通过类别设置阻止的 HTTPS 站点请求视为协议请求。因此，会显示协议阻止消息。HTTPS 请求也被记录为协议请求。

日志、状态消息和警报问题

在哪里查找 Websense 组件的错误消息？

当存在与 Websense 核心组件有关的错误或警告时，在 Websense Manager 中的**状态 > 今天**页面顶部的**运行状况警报摘要**中会显示简短警报消息（请参阅 *Websense 运行状况警报*，第 321 页）。

- 单击警报消息可在**状态 > 警报**页面查看更详细的信息。
- 在“状态”>“警报”页面单击消息旁边的**解决方案**可获取故障排除帮助。

来自 Websense 软件组件的错误、警告和消息以及数据库下载状态消息会被记录在 Websense **bin** 目录（默认情况下为 C:\Program Files\Websense\bin 或 /opt/Websense/bin）中的 **websense.log** 文件中。请参阅 *Websense 日志文件*，第 335 页。

对于安装在 Windows 计算机上的 Websense 软件组件，您还可以查看 Windows 事件查看器。请参阅 *Windows 事件查看器*，第 335 页。

Websense 运行状况警报

Websense 运行状况警报摘要列出了 Websense 软件的被监视组件所遇到的各种潜在问题。包括：

- Filtering Service 未在运行
- User Service 不可用
- Log Server 未在运行
- 没有为 Policy Server 配置 Log Server
- 日志数据库不可用
- Network Agent 未在运行
- 没有为 Policy Server 配置 Network Agent
- 没有为 Network Agent 配置监视 NIC
- 没有为 Network Agent 配置 Filtering Service
- 正在使用初始筛选数据库
- 正在首次下载主数据库
- 正在更新主数据库
- 主数据库是一周以前的
- 主数据库没有成功下载
- 未启用 WebCatcher

- 存在订购问题
- 订购密钥即将过期
- 未输入任何订购密钥

“警报”页面提供关于任何错误或警告条件的基本信息。单击**解决方案**了解有关解决问题的信息。

在某些情况下，如果您正在收到关于未使用组件或已禁用组件的错误或状态消息，您可以选择隐藏警报消息。请参阅*查看当前系统状态*，第 245 页，以了解更多信息。

为一个请求生成了两个日志记录

当 Windows QoS Packet Scheduler 与 Network Agent 安装在同一台计算机上时，会为每个从 Network Agent 计算机发出的 HTTP 或协议请求记录两个请求。（对于由网络内客户端计算机发出的请求不会出现这种重复记录的情况。）

要解决该问题，请在 Network Agent 计算机上禁用 Windows QoS Packet Scheduler。

如果使用 Network Agent 进行所有日志记录，则不会出现此问题。有关详细信息，请参阅*配置 NIC 设置*，第 292 页。

Policy Server 和 Policy Database 问题

- *忘记密码*，第 322 页
- *无法登录 Policy Server*，第 323 页
- *Websense Policy Database 服务无法启动*，第 323 页

忘记密码

如果您是超级管理员或使用 Websense 用户帐户通过 Websense Manager 登录 Policy Server 的委派管理员，则任何无限制超级管理员都可以重置密码。

- WebsenseAdministrator 密码是在**设置 > 帐户**页面设置的。
- 其他管理员帐户密码是在**委派管理 > 管理 Websense 用户帐户**页面设置的。

如果您没有使用委派管理，且忘记了 WebsenseAdministrator 密码，请登录 MyWebsense 以重置密码。

- 与 MyWebsense 帐户相关联的订购密钥必须与您当前的 Websense Web Security 或 Websense Web Filter 订购密钥匹配。
- 如果您有多个订购密钥，则必须选择相应的 Websense Web Security 或 Websense Web Filter 密钥，才能成功完成密码重置。
- 您必须拥有访问 Websense Manager 计算机的权限才能完成重置过程。

无法登录 Policy Server

请验证选定的 Policy Server IP 地址是否正确无误。如果 Policy Server 计算机的地址在 Policy Server 被添加到 Websense Manager 时被更改，您需要登录到其他 Policy Server，从 Websense Manager 删除旧 IP 地址，然后添加新的 Policy Server IP 地址。请参阅*添加并编辑 Policy Server 实例*，第 232 页。

如果 Websense Manager 突然停止，或通过 kill (Linux) 或 End Task (Windows) 命令停止，请等待几分钟，然后再次登录。 Websense 软件会在 3 分钟之内检测并关闭终止的会话。

Websense Policy Database 服务无法启动

Websense Policy Database 作为特殊帐户运行：**WebsenseDBUser**。如果此帐户遇到登录问题，则 Policy Database 会无法启动。

要解决此问题，请更改 WebsenseDBUser 密码。

1. 以本地管理员身份登录 Policy Database 计算机。
2. 转至**开始 > 程序 > 管理工具 > 计算机管理**。
3. 在导航窗格的“系统工具”下面，展开**本地用户和组**，然后选择**用户**。用户信息将显示在内容窗格中。
4. 右键单击 **WebsenseDBUser** 并选择**设置密码**。
5. 输入此用户帐户的新密码并确认，然后单击**确定**。
6. 关闭“计算机管理”对话框。
7. 转至**开始 > 程序 > 管理工具 > 服务**。
8. 右键单击 **Websense Policy Database** 并选择**属性**。
9. 在“属性”对话框的“登录”选项卡上，输入新的 WebsenseDBUser 密码信息，然后单击**确定**。
10. 再次右键单击 Websense Policy Database，然后选择**启动**。

    当服务启动后，关闭“服务”对话框。

委派管理问题

无法从角色中删除受管理客户端

在下列情况下，无法直接从“委派管理”>“编辑角色”页面的受管理客户端列表中删除客户端：

- 管理员已将策略应用于客户端
- 管理员已将一个策略应用于网络、组、域或组织单位的一个或多个成员

如果超级管理员在登录 Websense Manager 时没有选择与包含要删除客户端的目录服务进行通讯的 Policy Server，而选择了其他的 Policy Server，也可能会引发问题。在这种情况下，当前 Policy Server 和目录服务将不会识别客户端。

有关删除受管理客户端的帮助，请参阅*删除受管理客户端*，第 219 页。

登录错误显示其他人正在登录我的计算机

在尝试登录 Websense Manager 时，有时会收到错误“登录失败。在计算机 127.0.0.1 上，从 < 日期，时间 > 开始，角色 < 角色名称 > 已被 < 用户名 > 使用”。IP 地址 127.0.0.1 也被称为环回地址，通常表示本地计算机。

此消息表示，某人正在使用您请求的角色登录 Websense Manager 安装计算机。您可以选择其他角色（如果您管理多个角色）仅出于报告目的进行登录，或等待其他管理员注销后登录。

一些用户无法访问未筛选 URL 列表中的站点

未筛选的 URL 只会影响在其中添加 URL 的角色所管理的客户端。例如，如果超级管理员添加未筛选的 URL，则由委派管理角色所管理的客户端将无权访问这些站点。

要使站点可供其他角色中的客户端使用，超级管理员可以切换到每个角色并将相关站点添加到该角色的未筛选 URL 列表中。

重新分类的站点被根据错误的类别进行筛选

重新分类的 URL 只会影响在其中添加 URL 的角色所管理的客户端。例如，当超级管理员重新分类 URL 时，由委派管理角色所管理的客户端将继续根据这些站点的主数据库类别进行筛选。

要使重新分类适用于其他角色中的客户端，超级管理员可以切换到每个角色并为该角色重新分类站点。

无法创建自定义协议

只有超级管理员可以创建自定义协议。但是，委派管理员可以为自定义协议设置筛选操作。

当超级管理员创建自定义协议时，他们应当为大多数客户端设置合适的默认操作。然后，通知新协议的委派管理员，以便他们可以根据需要为他们的角色更新筛选器。

报告问题

Log Server 未在运行

如果 Log Server 未在运行，或其他 Websense 组件无法与 Log Server 进行通讯，则不会存储 Internet 使用信息，而且您将无法生成 Internet 使用报告。

在下列情况下， Log Server 不可用：

- Log Server 计算机上的磁盘空间不足。
- 您更改了 Microsoft SQL Server 或 MSDE 密码而没有更新 ODBC 或 Log Server 配置。
- 主数据库成功下载后已超过 14 天。
- logserver.ini file 文件丢失或损坏。
- 您为避免记录 Internet 使用信息而停止了 Log Server。

要对这些问题进行故障排除：

- 验证可用磁盘空间大小，并根据需要删除无关的文件。
- 如果您认为密码更改是导致问题的原因，请参阅*更新 Log Server 连接密码*，第 329 页。
- 转至 Websense **bin** 目录（默认情况下为 C:\Program Files\Websense\bin），确保您可以在文本编辑器中打开 **logserver.ini**。如果此文件已被损坏，请用备份文件将其替换。
- 查看 “Windows 服务”对话框以验证 Log Server 已启动，并在需要时重新启动服务 （请参阅*停止和启动 Websense 服务*，第 238 页）。
- 查看 Windows 事件查看器和 **websense.log** 文件以了解来自 Log Server 的错误消息 （请参阅*故障排除工具*，第 334 页）。

没有为 Policy Server 安装 Log Server

Websense Log Server 收集 Internet 使用信息并将其存储在日志数据库中，以供在调查报告、演示报告，以及 Websense Manager 中的 “今天”和 “历史”页面上的图表和摘要中使用。

必须安装 Log Server 才能进行报告。

在下列情况下，您可能会看到此消息：

- Log Server 与 Policy Server 安装在不同的计算机上，且 Websense Manager 中没有正确地将 Log Server IP 地址设置为本地主机。
- Log Server 安装在 Linux 计算机上。
- 没有使用 Websense 报告工具。

要验证 Websense Manager 中设置了正确的 Log Server IP 地址：

1. 选择左侧导航窗格的**设置**选项卡，然后转至**常规 > 记录**。
2. 在 **Log Server IP 地址或名称**字段输入 Log Server 计算机的 IP 地址。
3. 单击**确定**以缓存更改，然后单击**全部保存**。

如果 Log Server 安装在 Linux 计算机上，或者没有使用 Websense 报告工具，则可以在 Websense Manager 中隐藏警报消息。

1. 在左侧导航窗格的 “主要”选项卡上，转至**状态 > 警报**。
2. 在 “活动警报”下，单击**高级**。
3. 对 “没有安装 Log Server”消息勾选**隐藏此警报**。
4. 单击**立即保存**。更改会立即实施。

未创建日志数据库

有时，安装程序无法创建日志数据库。以下列表描述了常见的原因和解决方案。

问题：	存在使用 Websense 软件用于日志数据库的名称的文件（wslogdb70 和 wslogdb70_1），但这些文件未被正确地连接到数据库引擎，所有无法被 Websense 安装程序使用。
解决方案：	删除或重命名现有文件，然后再次运行安装程序。
问题：	为安装而登录的帐户在安装数据库的驱动器上的权限不足。
解决方案：	将登录帐户更新为具有对安装位置的读写权限，或使用已经具有这些权限的其他帐户登录。然后，再次运行安装程序。
问题：	指定位置的可用磁盘空间不足，无法创建和维护日志数据库。
解决方案：	在选定的磁盘上清空足够的空间以安装和维护日志数据库。然后，再次运行安装程序。也可以选择其他位置。
问题：	为安装而登录的帐户没有足够的 SQL Server 权限来创建数据库。
解决方案：	更新登录帐户或使用已经具有所需权限的帐户登录。然后，再次运行安装程序。 所需权限取决于 Microsoft SQL Server 的版本： ■ SQL Server 2000 或 MSDE：需要 **dbo** （数据库所有者）权限 ■ SQL Server 2005：需要 **dbo** 和 **SQLServerAgentReader** 权限

日志数据库不可用

Websense 日志数据库存储 Internet 使用信息，以供在演示报告、调查报告，以及 Websense Manager “今天”和“历史”页面上的图表和摘要中使用。

如果 Websense 软件无法连接日志数据库，请首先验证数据库引擎（Microsoft SQL Server 或 Microsoft SQL Server Desktop Engine [MSDE]）正在日志数据库计算机上运行。

1. 打开 “Windows 服务”对话框 （请参阅 *Windows 服务对话框*，第 334 页）并验证下列服务正在运行：
   - Microsoft SQL Server：
     - MSSQLSERVER
     - SQLSERVERAGENT
   - Microsoft SQL Desktop Engine (MSDE)：
     - MSSQL$WEBSENSE （如果您是从 Websense, Inc. 获取 MSDE）
     - SQLAgent$WEBSENSE

2. 如果某项服务已停止，请右键单击服务名，然后单击**启动**。

   如果服务没有重新启动，请检查 Windows 事件查看器（请参阅 *Windows 事件查看器*，第 335 页）以查看 Microsoft SQL Server 或 MSDE 错误和警告。

如果数据库引擎正在运行：

- 请确保 SQL Server Agent 正在运行数据库引擎的计算机上运行。
- 请使用 “Windows 服务”对话框确保 **Websense Log Server** 服务正在运行。
- 如果 Log Server 和日志数据库位于不同的计算机上，请确保两个计算机都在运行，且计算机之间的网络连接没有受损。
- 请确保日志数据库计算机上有足够的磁盘空间，且日志数据库具有足够数量的已分配磁盘空间（请参阅 *Log Server 未在日志数据库中记录数据*，第 328 页）。
- 请确保 Microsoft SQL Server 或 MSDE 密码未被更改。如果密码发生了更改，您必须更新 Log Server 用于连接数据库的密码信息。请参阅*更新 Log Server 连接密码*，第 329 页。

日志数据库大小

日志数据库大小始终都很重要。如果您成功地生成了 Websense 报告但注意到现在显示报告要等待较长时间，或您开始从网络浏览器收到超时消息，请考虑禁用某些数据库分区。

1. 在 Websense Manager 中，转至**设置 > 报告 > 日志数据库**。
2. 找到该页的**可用分区**部分。
3. 清除当前报告操作不需要的所有分区的**启用**复选框。
4. 单击**立即保存**以执行更改。

Log Server 未在日志数据库中记录数据

通常，当 Log Server 无法将数据写入日志数据库时，就表明数据库超出了所分配的磁盘空间。在磁盘驱动器已满，或在 Microsoft SQL Server 中没有为数据库容量可以增长的大小设置最大值时，会出现这种情况。

如果存放日志数据库的磁盘驱动器已满，则您必须向计算机增加磁盘空间以恢复记录。

如果您的 SQL Server 数据库管理员已为 Microsoft SQL Server 中的单个数据库的容量设置了可以增长的最大大小，请执行下列操作之一：

- 联系 SQL Server 数据库管理员以增加最大大小。
- 查明最大大小，然后转至**设置 > 报告 > 日志数据库**，将日志数据库配置为达到最大大小的大约 90% 时进行翻转。请参阅*配置翻转选项*，第 272 页。

如果您的信息技术部门已经为 SQL Server 操作建立了最大磁盘空间，请联系他们以寻求帮助。

更新 Log Server 连接密码

如果您更改了 Websense 软件用来连接到日志数据库的帐户的密码，您也必须更新 Log Server 为使用新密码。

1. 在 Log Server 计算机上，转至**开始 > 程序 > Websense > 实用程序 > Log Server 配置**。打开 Log Server 配置实用程序。
2. 单击**数据库**选项卡，然后验证在“ODBC 数据源名称 (DSN)”字段中显示了正确的数据库 （默认情况下为 **wslogdb70**）。
3. 单击**连接**。将打开 “选择数据源”对话框。
4. 单击**计算机数据源**选项卡，然后双击 **wslogdb70**（或您的日志数据库名称）。将打开 “SQL Server 登录”对话框。
5. 确保 LoginID 字段包含正确的帐户名 （通常为 **sa**），然后输入新密码。
6. 单击**确定**，然后在 “Log Server 配置”对话框中，单击**应用**。
7. 单击**连接**选项卡，然后停止 Log Server 并重新启动。
8. 当 Log Server 再次运行时，单击**确定**关闭实用程序。

配置 Microsoft SQL Server 2005 的用户权限

Microsoft SQL Server 2005 对 SQL Server Agent 角色的定义为管理作业框架的可访问性。SQL Server 2005 的 SQL Server Agent 作业储存在 SQL Server msdb 数据库中。

要成功安装 Websense Log Server，拥有 Websense 数据库的用户帐户必须在 msdb 数据库中有以下角色资格之一：

- SQLAgentUser 角色
- SQLAgentReader 角色
- SQLAgentOperator 角色

> **注意**
> SQL 用户帐户还必须是 DBCreator 固定式服务器角色的成员。

请前往 Microsoft SQL Server 2005 以授予成功安装 Websense 报告组件所需的 SQL Server 用户帐户权限。

1. 在 SQL Server 计算机上，进入**开始 > 程序 > Microsoft SQL Server 2005 > Microsoft SQL Server Management Studio**。
2. 选择 **Object Explorer** 树。
3. Select **安全 > 登录**。
4. 选择安装时所用的登录帐户。
5. 右键点击登录帐户并为该用户选择**属性**。

6. 选择**用户映射**并执行以下操作：
   a. 在数据库映射中选择 **msdb**。
   b. 向以下角色之一授予资格：
      - SQLAgentUser 角色
      - SQLAgentReader 角色
      - SQLAgentOperator 角色
   c. 单击**确定**以保存。
7. 选择**服务器角色**，然后选择 **dbcreator**。此时 dbcreator 角色创建成功。
8. 单击**确定**以保存。

Log Server 无法连接到目录服务

如果出现了下面的错误之一， Log Server 将无法访问目录服务，而这对于报告时更新用户与组的映射是必需的。这些错误会显示在 Windows 事件查看器中（请参阅 *Windows 事件查看器*，第 335 页）。

- EVENT ID:4096 – 无法初始化目录服务。Websense Server 可能已宕机或无法访问。
- EVENT ID:4096 – 无法连接到目录服务。目前将不会解析此用户的组。请验证该进程可访问目录服务。

最常见的原因是 Websense Log Server 和 Websense User Service 位于限制访问的防火墙的不同侧。

要解决此问题，请将防火墙配置为允许通过用于这些组件之间通讯的端口进行访问。

Internet 浏览时间报告上的数据出现偏差

请注意，合并可能会导致 Internet 浏览时间报告中的数据出现偏差。这些报告将显示用户在访问 Internet 时花费的时间，并可以包含在每个站点上所花费时间的详细信息。Internet 浏览时间是采用一种特殊算法计算而得，允许合并可能会降低这些报告的计算准确度。

带宽大于预期

许多（但并非全部）Websense 集成产品会提供带宽信息。如果您的集成产品没有提供带宽信息，您可以将 Network Agent 配置为执行日志记录，从而包括带宽数据。

当用户请求允许的文件下载时，集成产品或 Network Agent 将发送完整的文件大小， Websense 软件会将其记录为接收的字节。

如果用户随后取消了实际下载，或文件没有完全下载，则日志数据库中接收的字节值仍然代表完整文件大小。在这些情况下，报告的接收字节值将大于实际接收的字节数。

这还会影响报告的带宽值，它表示接收字节和发送字节的组合。

一些协议请求未被记录

一些协议（例如 ICQ 和 AOL 使用的协议）会提示用户登录使用一个 IP 地址的服务器，然后出于发送消息的目的将不同的识别 IP 地址和端口号发送到客户端。在这种情况下，发送和接收的所有消息可能都不会被 Websense Network Agent 监视和记录，因为消息服务器在交换消息时是未知的。

因此，记录的请求数量与实际发送请求的数量可能不匹配。这会影响 Websense 报告工具生成的报告的准确度。

所有报告均为空

如果您的所有报告都没有数据，请确保：

- 活动数据库分区包括报告中所包含的日期信息。请参阅*数据库分区*，第 331 页。
- SQL Server Agent 作业在 Microsoft SQL Server 或 MSDE 中处于活动状态。请参阅 *SQL Server Agent 作业*，第 331 页。
- Log Server 被正确地设置为接收来自 Filtering Service 的日志信息。请参阅 *Log Server 配置*，第 332 页。

数据库分区

Websense 日志记录存储在数据库中的分区中。您可以根据大小和日期创建新分区，具体取决于您的数据库引擎和配置。

您可以在 Websense Manager 中激活或停用独立分区。如果您尝试根据存储在已停用分区中的信息生成报告，将不会找到任何信息且报告为空。

要确保合适的数据库分区处于活动状态：

1. 转至**设置 > 报告 > 日志数据库**。
2. 向下滚动至**可用分区**部分。
3. 对于含有报告中所需包括的数据的每个分区，勾选**启用**复选框。
4. 单击**立即保存**以执行更改。

SQL Server Agent 作业

SQL Server Agent 数据库作业可能已被禁用。必须运行此作业，ETL 数据库作业才能将日志记录处理加入数据库中。

如果您正在运行 MSDE：

1. 请转至**开始 > 管理工具 > 服务**。
2. 确保 SQL Server 和 SQL Server Agent 服务都已启动。如果您是从 Websense, Inc. 获取 MSDE，则这些服务被称为 MSSQL$WEBSENSE 和 SQLAgent$WEBSENSE。

如果您正在运行完整的 Microsoft SQL Server，请要求您的数据库管理员确保 SQL Server Agent 作业正在运行。

Log Server 配置

Websense Manager 和 Log Server 中的配置设置必须正确，才能确保 Log Server 接收来自 Filtering Service 日志信息。否则，日志数据将不会被处理加入日志数据库。

首先，请验证 Websense Manager 是否成功连接到 Log Server。

1. 使用无限制超级管理员权限登录 Websense Manager。
2. 转至**设置 > 常规 > 记录**。
3. 输入 Log Server 所在的**计算机名称**或 **IP 地址**。
4. 输入 Log Server 正在侦听的**端口**（默认情况下为 55805）。
5. 单击**检查状态**以确定 Websense Manager 是否能够与特定的 Log Server 进行通讯。

   将出现一条消息，表明连接是否通过测试。更新 IP 地址或计算机名称和端口（如需要），直到测试成功为止。
6. 完成之后，请单击**确定**以缓存您的更改。直到您单击**全部保存**之后，更改才会生效实施。

接下来，验证 Log Server 配置实用程序中的设置。

1. 在运行 Log Server 的计算机上，转至**开始 > 程序 > Websense > 实用程序 > Log Server 配置**。
2. 在**连接**选项卡上，验证端口是否与在 Websense Manager 中输入的值相匹配。
3. 单击**确定**以保存更改。
4. 使用**连接**选项卡上的按钮停止，然后启动 Log Server。
5. 单击**退出**关闭 Log Server 配置实用程序。

在“今天”或“历史”页面上没有显示任何图表

在使用委派管理的组织中，查看委派管理员的角色的报告权限。如果**查看今天和历史页上的报告**未选中，则不会向该角色中的委派管理员显示这些图表。

在使用多个 Policy Servers 的环境中，Log Server 被安装为仅与一个 Policy Server 进行通讯。您必须登录到 Policy Server 查看“今天”和“历史”页面上的图表，或访问其他报告功能。

无法访问某些报告功能

如果您的网络浏览器采用了非常严格的弹出窗口拦截设置，它可能会阻止某些报告功能。要使用这些功能，您必须降低拦截级别或完全禁用弹出窗口拦截。

Microsoft Excel 输出缺少某些报告数据

在 Microsoft Excel 工作表中可打开的最大行数为 65,536。如果您将超过 65,536 个记录的报告导出为 Microsoft Excel 格式，则第 65,537 行及以后的记录在工作表中不可用。

要确保访问导出报告中的所有信息，请执行下列操作之一：

- 对于演示报告，请编辑报告筛选器以定义较小的报告，可行的办法有：设置较短的日期范围、选择较少的用户和组，或选择较少的操作。
- 对于调查报告，请进一步查看数据以定义一个较小的报告。
- 选择其他导出格式。

将演示报告输出保存为 HTML

如果您直接从报告 > 演示报告页面生成报告，您有 3 种显示格式可供选择：HTML、PDF 和 XLS。如果您选择 HTML 显示格式，则可以在 Websense Manager 窗口中查看报告。

不推荐从浏览器打印和保存演示报告。打印输出中包括整个浏览器窗口，且打开保存的文件会启动 Websense Manager。

为了更有效地保存报告，请选择 PDF 或 XLS 作为输出格式。如果本地计算机上安装了查看软件（Adobe Reader 或 Microsoft Excel），您可以立即打开这些文件类型。您也可以将文件保存到磁盘（在合适的查看软件不可用时的唯一选项）。

在 Adobe Reader 或 Microsoft Excel 中打开报告之后，可使用该应用程序的打印和保存选项来生成所需的最终输出。

调查报告搜索问题

有两个与搜索调查报告有关的潜在问题。

- 无法输入展开的 ASCII 字符
- 找不到搜索模式

展开的 ASCII 字符

主调查报告页面条形图上方的 “搜索”字段让您能够在所选择的图表元素中搜索具体的词汇或文本字符串。

如果您正在 Linux 服务器上使用 Mozilla Firefox 来访问 Websense Manager，则无法在这些字段中输入展开的 ASCII 字符。这是 Firefox 在 Linux 上的一个已知限制。

如果您需要在调查报告中搜索包含展开 ASCII 字符的文本字符串，请使用任何受支持的浏览器从 Windows 服务器访问 Websense Manager。

未找到搜索模式

有时，调查报告无法找到与在调查报告主页面上的“搜索”字段中所输入的模式相关的 URL。如果出现这种情况，且您有充分理由确定该模式存在于所报告的 URL 中，请尝试输入也可能找到所需 URL 的其他模式。

常见调查报告问题

- 某些查询会需要很长时间。您可能会看到空白屏幕或收得一条表明您的查询已超时的消息。出现这种情况有下列原因：
  - Web 服务器超时
  - MSDE 或 Microsoft SQL Server 超时
  - 代理或缓存服务器超时

  您可能需要手动增加这些组件的超时限制。
- 如果用户不属于任何组，他们也不会显示在域中。组和域选项都将处于非活动状态。
- 即使 Log Server 正在记录访问量而不是点击量，调查报告也会将此信息标记为**点击量**。

故障排除工具

- *Windows 服务对话框*，第 334 页
- *Windows 事件查看器*，第 335 页
- *Websense 日志文件*，第 335 页

Windows 服务对话框

在 Microsoft Windows 计算机上，Filtering Service、Network Agent、Policy Server、User Service 和所有 Websense 透明标识代理均作为服务运行。您可以使用“Windows 服务”对话框来查看这些服务的状态。

1. 在 Windows 控制面板中，打开**管理工具**文件夹。
2. 双击**服务**。
3. 滚动服务列表，找到要进行故障排除的服务。

   服务项包括服务名称、简短服务描述、服务状态（已启动或已停止）、如何启动服务，以及服务使用哪个帐户执行其任务。
4. 双击服务名称可打开属性对话框，其中包含了关于服务的更多详细信息。

Windows 事件查看器

Windows 事件查看器记录了有关 Windows 事件的错误消息，其中包括服务活动。这些消息可帮助您确定可能导致 Internet 筛选或用户标识问题的网络或服务错误。

1. 在 Windows 控制面板中，打开**管理工具**文件夹。
2. 双击**事件查看器**。
3. 在事件查看器中，单击**应用程序**可获得有关错误消息、警告和信息消息的列表。
4. 滚动列表以确认来自 Websense 服务的错误或警告。

Websense 日志文件

Websense 软件将错误消息写入 **websense.log** 文件，它位于 Websense **bin** 目录（默认情况下为 C:\Program Files\Websense\bin 或 /opt/Websense/bin）中。

此文件中的信息与 Windows 事件查看器中的信息类似。在 Windows 环境中，事件查看器能够以更加用户友好的格式显示消息。但是，**websense.log** 文件可用于 Linux 系统，并且能够在您需要问题故障排除帮助时被发送给 Websense 技术支持。

索引

D

H

I

J

Q

R

S

X

Y

Z