FireSIGHT 用户代理配置指南

版本 2.2
2014 年 6 月 23 日

思科系统公司
www.cisco.com
思科在全球设有 200 多个办事处。
有关地址、电话号码和传真号码信息，
可查阅思科网站：
www.cisco.com/go/offices。

目 录

简介

用户代理版本 2.2 与 FireSIGHT 系统受管设备配合工作以收集用户数据。如果将代理与 FireSIGHT 系统 5.x 版本配合使用，则用户代理对于实施用户访问控制也非常重要。

用户代理监控 Microsoft Active Directory 服务器并报告通过 LDAP 验证的用户登录和注销。FireSIGHT 系统将这些记录与其通过直接网络流量观察 （按受管设备）收集到的信息整合到一起。

有关详细信息，请参阅以下各节：

用户代理版本 2.2 的主要更改

如果要将用户代理升级至版本 2.2，请注意以下更改：

- 将用户代理 2.0 版本升级到 2.1.1 版本时，必须备份数据库以保留现有的配置设置。有关详情，请参见备份用户代理配置，第 2-7 页。

  但是，版本 2.2 版本的代理会为未来升级自动保留配置设置。如果卸载并重新安装版本 2.2 版本的代理，则无需手动备份数据库。
- 代理能够检测到已配置 Active Directory 服务器的用户登录。配置连接时，请从 **Local Login IP Address** 字段选择一个 IP 地址。
- 已配置的 Active Directory 服务器连接支持最多 64 个字符的用户密码。
- 代理当前支持的 **Active Directory Server Max Poll Length** 为 1 分钟和 5 分钟。使用更短的最大轮询时间可以提升实时监控性能和注销检测能力。

了解用户代理

本部分的概念重点介绍用户代理在 FireSIGHT 系统上实施用户发现中的作用。有关与用户发现和网络发现 （或 4.x 版本文档中的 RNA）相关的所有概念的详细讨论，请参阅设备上运行的 FireSIGHT 系统版本的《*FireSIGHT 系统用户指南*》。

有关详细信息，请参阅以下各节：

了解用户代理功能

FireSIGHT 系统可从贵公司的 LDAP 服务器获取用户身份和用户活动信息。通过用户代理，您可以在用户使用 Active Directory 凭证进行 Microsoft Active Directory 服务器身份验证时对用户进行监控。

您可以在通过 TCP/IP 访问 Microsoft Active Directory 服务器的所有 Microsoft Windows Vista、Microsoft Windows 7、Microsoft Windows 8、Microsoft Windows Server 2003、Microsoft Windows Server 2008、Microsoft Windows Server 2012 的计算机上安装代理。您也可以在运行任一受支持操作系统的 Active Directory 服务器上安装代理。

每个代理均可通过定期按计划轮询或实时监控来监控使用加密流量的登录。用户登录计算机时（无论是在工作站登录还是通过远程桌面登录）， Active Directory 服务器会生成登录。

代理还可以监控和报告用户注销情况。当检测到用户从主机 IP 地址注销时，代理会生成注销。当检测到登录主机的用户已更改时 （在 Active Directory 服务器报告用户已更改之前），代理也会生成注销。将注销数据与登录数据结合起来，便对登录到网络的用户有了更全面的了解。

轮询 Active Directory 服务器允许代理在定义的轮询时间间隔批量检索用户活动数据。一旦 Active Directory 接收到用户活动数据，实时监控就会将这些数据传输到代理。

可以配置代理，从而不报告与特定用户名或 IP 地址相关的任何登录或注销。这项配置很有用，例如，排除共享服务器上 （如文件共享和打印服务器）的重复登录，以及排除为排除故障登录计算机的用户。

每个代理可配置用来监控最多五个服务器，并将加密数据传输到最多五个防御中心。

代理将所有检测到的登录和注销 （不包括排除的用户名或 IP 地址）发送到防御中心，由其以用户活动的形式进行记录和报告。代理检测防御中心版本并以适当的数据格式发送登录记录。这可以补充受管设备直接检测到的用户活动。如果使用 5.x 版本的 FireSIGHT 系统执行访问控制，用户代理报告的登录将用户与 IP 地址相关联，从而允许触发包含用户条件的访问控制规则。

用户代理在用户登录网络或者帐户因其他原因使用 Active Directory 凭证进行身份验证时，对用户进行监控。版本 2.2 版本的用户代理对主机上的交互式用户登录、远程桌面登录、文件共享身份验证、计算机帐户登录、用户注销以及用户已从其注销的远程桌面会话进行检测。

检测到的登录类型将决定代理报告登录，以及主机配置文件中显示登录的方式。主机的*授权用户登录*会导致映射到主机 IP 地址的当前用户更改为新登录的用户。其他类型的登录不会更改主机的当前用户，或者仅当主机上的现有用户没有该主机的授权用户登录时，才会更改该主机的当前用户。在这些情况下，如果预期的用户不再处于登录状态，则会为该用户生成注销事件。仅在主机上的现有用户没有该主机的授权用户登录时，网络发现检测到的用户登录才会更改该主机的当前用户。代理检测到的登录对网络映射有下列影响：

- 当代理检测到用户对主机的交互式登录或检测到远程桌面登录时，该代理报告主机的授权用户登录并将主机的当前用户更改为新用户。
- 如果代理检测到使用文件共享身份验证的登录，则报告主机的用户登录活动，但不更改主机的当前用户。
- 如果代理检测到计算机帐户登录主机，则生成 NetBIOS 名称更改发现事件，主机配置文件也会反映对 NetBIOS 名称的更改。
- 如果代理检测到一个已排除用户名的登录活动，则不向防御中心报告此登录活动。

发生登录或其他身份验证活动时，代理会向防御中心发送以下信息：

- 用户的 LDAP 用户名
- 发生登录或其他身份验证的时间
- 用户主机的 IP 地址和本地链路地址 （如果代理报告了计算机帐户登录的 IPv6 地址）

注 如果用户使用一台 Linux 计算机通过远程桌面登录一台 Windows 计算机，一旦代理检测到此登录，就会向防御中心报告此 Windows 计算机的 IP 地址，而不是 Linux 计算机的 IP 地址。

防御中心将登录和注销消息记录为用户活动。当用户代理报告来自用户登录或注销的用户数据时，会将所报告的用户与用户列表进行比对。如果所报告的用户与代理所报告的现有用户匹配，报告的数据将分配给该用户。如果所报告的用户与现有用户不匹配，则会导致创建一个新用户。

即使不会报告与一个已排除用户名相关的用户活动，但可能仍将报告相关的用户活动。如果代理检测到用户登录机器，然后该代理检测到第二个用户登录，并且您已排除与第二次用户登录相关的用户名的报告，则代理会报告原始用户的注销。但是，不会报告第二个用户的登录活动。因此，不会将任何用户映射到 IP 地址，即使有排除的用户已登录主机。

请注意，代理检测到的用户名具有以下限制：

- 以美元符号字符 ($) 结尾的用户名被报告给 5.0.2 以上版本的防御中心以更新网络映射，但不会显示为用户登录。代理不向其他任何版本的防御中心报告以美元符号字符 ($) 结尾的用户名。
- 防御中心对包含 Unicode 字符的用户名显示可能有限制。

防御中心可存储的检测用户的总数取决于 RNA 或 FireSIGHT 许可证。如果达到许可的用户限制，多数情况下，系统会停止向数据库添加新用户。要添加新用户，须手动从数据库中删除旧的或不活动用户，或清除数据库中的所有用户。

了解旧版代理支持

安装在 Active Directory LDAP 服务器上的 1.0 版本的 （旧版）用户代理可以继续从 Active Directory 服务器向单个防御中心发送用户登录数据。旧版代理的部署需求和检测能力不变。须将这些代理安装在 Active Directory 服务器上连接到仅且一个防御中心。请注意，用户代理状态监控器运行状况模块不支持旧版代理，因此在连接了旧版代理的防御中心上不可启用该模块。在未来的版本中，对旧版代理的支持将逐步取消，因此，您应尽快升级部署，使用版本 2.2 用户代理。

了解 5.x 版本中的代理和访问控制

许可证：可控性

如果您的组织使用 Microsoft Active Directory LDAP 服务器， Cisco 建议您安装用户代理以通过 Active Directory 服务器监控用户活动。如果要在 5.x 版本中执行用户控制，**必须**安装并使用用户代理；代理将用户与 IP 地址相关联，从而允许触发包含用户条件的访问控制规则。可以使用一个代理来监控最多五个 Active Directory 服务器上的用户活动。

要使用代理，必须配置连接到代理的每个防御中心与监控的 LDAP 服务器之间的连接。此连接不仅允许检索用户代理检测到的登录和注销用户的元数据，还可用于指定在访问控制规则中使用的用户和组。有关为用户发现配置 LDAP 服务器的详细信息，请参阅《*FireSIGHT 系统用户指南*》。

注　在 Microsoft Active Directory 服务器上安装的旧版代理也会在用户使用 Active Directory 凭证进行身份验证时对用户进行监控。但是，您应尽快将用户代理迁移至版本 2.2，因为未来版本将不再支持旧版代理。

了解用户数据库

许可证：FireSIGHT

用户数据库包含受管设备或用户代理检测到的每个用户的记录。防御中心可存储的检测用户的总数取决于 FireSIGHT 许可证。在达到许可限制的用户数量后，大多数情况下，系统停止将新用户添加到数据库。要添加新用户，必须手动从数据库中删除旧的或非活动用户，或者清除数据库中的所有用户。

但是，系统会优先接受授权用户登录。如果已达到用户数量限制，并且系统检测到之前未检测到的用户的授权用户登录，系统将删除保持非活动状态时间最长的用户，并将其替换为新用户。

可以使用防御中心网络界面查看用户数据库的内容。有关查看、搜索和删除检测用户的信息，请参阅《*FireSIGHT 系统用户指南*》。

了解用户活动数据库

许可证：FireSIGHT

用户活动数据库包含网络中用户活动的记录，记录可来自受用户代理监控的 Active Directory LDAP 服务器的连接或是通过网络发现得到。系统会在以下情况下记录事件：

- 系统检测到单独的登录或注销
- 系统检测到新用户
- 您手动删除用户
- 系统检测到不在数据库中的用户，但因已达到 FireSIGHT 许可限制而无法添加该用户

可使用防御中心网络界面查看系统检测到的用户活动。有关查看、搜索和删除用户活动的信息，请参阅《*FireSIGHT 系统用户指南*》。如果要使用版本 2.2 FireSIGHT 系统用户代理将 LDAP 登录数据发送到 5.x 版本防御中心，必须为每个代理在您希望代理连接的每个防御中心上配置一个连接。该连接允许代理建立一个与防御中心之间的安全连接，代理可以通过此连接发送登录数据。如果代理配置为排除特定用户名，那么这些用户名的登录数据不会报告给 防御中心。

此外，如果您正计划实施用户访问控制，则必须设置至您计划收集数据的每个 Microsoft Active Directory 服务器的连接，并配置用户感知参数。

了解访问受控用户数据库

许可证：可控性

访问受控用户数据库包含可在访问控制规则中使用的用户和组，因此，可使用 FireSIGHT 系统执行用户控制。这些用户可以是以下两种类型之一：

- *访问受控用户*为可以添加到访问控制规则以执行用户控制的用户。在配置防御中心与 LDAP 服务器的连接时，可指定访问受控用户必须所属的组。
- *非访问受控用户*是任何其他被检测到的用户。

防御中心可存储的访问受控用户的总数取决于您拥有的 FireSIGHT 许可证。

在配置防御中心与 LDAP 服务器的连接时，可指定访问受控用户必须所属的组，如《*FireSIGHT 系统用户指南*》中所述。

如果要使用版本 2.2 FireSIGHT 系统用户代理将 LDAP 登录和注销数据发送到 5.x 版本防御中心，必须为每个代理在您希望代理连接的每个防御中心上配置一个连接。该连接允许代理在与防御中心之间建立一个安全的连接，代理可以通过此连接发送用户活动数据。

如果代理配置为排除特定用户名，那么这些用户名的用户活动数据将不会报告给防御中心。这些已排除的用户名仍保留在数据库中，但不与 IP 地址关联。

此外，如果您正计划实施用户访问控制，则必须设置至您计划收集数据的每个 Microsoft Active Directory 服务器的连接，并配置用户感知参数。

用户数据收集限制

许可证：FireSIGHT

下表介绍用户数据收集常规限制或与代理相关的特定限制。

表 1-1　　用户数据收集限制

限制	描述
用户控制	要执行用户控制，组织**必须**使用 Microsoft Active Directory LDAP 服务器。系统从 Active Directory 获取可在访问控制规中使用的用户和组，并使用安装在 Active Directory 服务器上的用户代理所报告的登录和注销数据将用户与 IP 地址进行绑定。
登录检测	代理将带有 IPv6 地址的主机上的用户登录报告给运行 5.2+ 版本的防御中心。 代理将未授权用户登录和 NetBIOS 登录报告给运行 5.0.1+ 版本的防御中心。 代理会将实际用户名的授权登录报告给运行 4.10.x 版本的防御中心。 如果要检测 Active Directory 服务器上的登录，必须用服务器 IP 地址配置 Active Directory 服务器连接。有关详细信息，请参阅配置用户代理与 Active Directory 服务器间的连接，第 2-9 页。 如果有多个用户使用远程会话登录主机，代理可能无法正常检测到该主机上的登录。有关防止这种情况的详细信息，请参阅启用空闲会话超时，第 2-5 页。
注销检测	代理会将检测到的注销报告给版本 5.2 以上的防御中心。 注销可能不会立即被检测到。与注销关联的时间戳是代理检测到用户不再映射到主机 IP 地址的时间，此时间可能与用户注销主机的实际时间不一致。 当检测到用户从主机 IP 地址注销时，代理会生成注销。当检测到登录主机的用户已更改时 （在 Active Directory 服务器报告用户已更改之前），代理也会生成注销。
实时数据检索	Active Directory 服务器必须运行 Windows Server 2008 或 Windows Server 2012。
不同用户多次登录到同一主机	系统假设一次只有一个用户登录任何给定主机，且主机的当前用户是最后一次授权用户登录。如果只有未授权登录用户登录到主机，最后的未授权登录用户将被视为当前用户。如果有多个用户通过远程会话登录， Active Directory 服务器报告的最后用户是报告给防御中心的用户。

表 1-1　用户数据收集限制 （续）

限制	描述
同一用户多次登录到同一主机	系统记录用户在特定主机的首次登录并忽略后续的登录。如果单个用户是唯一登录到特定主机的人员，则系统唯一记录的登录为原始登录。 然而，如果另一用户登录到该主机，则系统会记录新的登录。如果原始用户再次登录，将会记录其新的登录。
Unicode 字符	用户界面可能无法正确显示包含 Unicode 字符的用户名。 代理不会将包含 Unicode 字符的用户名报告给版本 4.10.x 防御中心。
用户数据库中的 LDAP 用户帐户	如果从用户感知或 RUA LDAP 服务器上删除或禁用一个 LDAP 用户，或排除此用户名向防御中心报告，则防御中心不会从用户数据库中删除该用户，该用户继续被算在数据库所列用户许可数量限制内。必须从数据库中手动清除该用户。请注意，对于版本 5.x，用户许可证限制对访问受控用户同时应用；访问受控用户的用户数取决于 LDAP 配置检索到的用户数量。

设置用户代理

要通过用户代理版本 2.2 从 Microsoft Active Directory 服务器收集用户登录数据并将其发送给防御中心，必须安装用户代理，将其连接到每个防御中心和 Microsoft Active Directory 服务器，并配置常规设置。

要设置用户代理，请执行以下操作：

访问权限：管理员

步骤 1 配置每个防御中心以从将安装代理的计算机的 IP 地址进行连接。有关详情，请参阅：

- 准备连接到 4.x 版本的防御中心，第 2-2 页
- 准备连接到 5.x 版本的防御中心，第 2-2 页

注 如果要使用 5.x 版本的防御中心执行用户控制，还必须配置防御中心上到 Microsoft Active Directory 服务器的 LDAP 连接 （具有用户感知参数）。

步骤 2 配置代理连接到 Active Directory 服务器时所需的 Windows 和用户权限。有关详细信息，请参阅配置权限以连接到 Active Directory 服务器，第 2-4 页。

步骤 3 或者，对空闲远程会话启用超时。有关详细信息，请参阅启用空闲会话超时，第 2-5 页。

步骤 4 在将安装代理的计算机上安装所需程序。设置计算机对 Active Directory 服务器的 TCP/IP 访问。有关详细信息，请参阅配置权限以连接到 Active Directory 服务器，第 2-4 页。

步骤 5 或者，备份代理数据库以保留用户代理先前版本的配置设置。有关详细信息，请参阅备份用户代理配置，第 2-7 页。

步骤 6 在计算机上安装代理。有关详细信息，请参阅安装用户代理，第 2-7 页。

步骤 7 配置连接，将代理连接到最多五个 Microsoft Active Directory 服务器。或者，配置代理的轮询间隔和最大轮询时间。有关详细信息，请参阅配置用户代理与 Active Directory 服务器间的连接，第 2-9 页。

步骤 8 配置连接，将代理连接到最多五个防御中心。有关详细信息，请参阅配置用户代理防御中心连接，第 2-12 页。

步骤 9 或者，配置从轮询登录和注销数据中排除的用户名和 IP 地址列表。有关详细信息，请参阅配置用户代理排除用户名设置，第 2-13 页和配置用户代理排除地址设置，第 2-14 页。

步骤 10 或者，配置代理日志记录设置。有关详细信息，请参阅配置用户代理日志记录设置，第 2-14 页。

步骤 11 或者，配置代理名称，启动和停止服务，并查看服务的当前状态。有关详细信息，请参阅配置常规用户代理设置，第 2-16 页。

步骤 12　点击 **Save**，保存代理配置。

注意　除非技术支持指示您修改代理维护设置，否则请**勿**擅自修改。

准备连接到 4.x 版本的防御中心

通过用户代理收集 LDAP 用户登录信息的第一步，配置每个防御中心，以允许来自用于连接 Active Directory 服务器的代理的连接。本节介绍在 4.x 版本的防御中心上授权代理连接的步骤。

要配置防御中心以连接到用户代理，请执行以下操作：

访问权限：管理员

步骤 1　选择 **Operations > Configuration > RUA**。

步骤 2　点击 **Add RUA Agent**。

步骤 3　在 **Name** 字段中，键入一个代理的描述性名称。

步骤 4　在 **Hostname or IP Address** 字段中键入用户代理驻留的计算机的 IP 地址或主机名。必须使用 IPv4 地址；若使用 IPv6 地址，您**将无法**配置防御中心连接到用户代理。

注　您无法添加使用 IPv6 地址的用户代理或解析为 IPv6 地址的主机名。

步骤 5　点击 **Add RUA Agent**。

防御中心配置为允许来自该 IP 地址的代理发起的连接。

提示　要删除防御中心与代理之间的连接，请点击待删除的连接旁边的 **Delete**。

步骤 6　继续执行配置权限以连接到 Active Directory 服务器，第 2-4 页。

准备连接到 5.x 版本的防御中心

如果您想要使用用户代理的版本 2.2 版本发送 LDAP 登录数据到 5.x 版本的防御中心，必须在代理待连接到的每个防御中心上为每个代理配置连接。该连接允许代理在与防御中心之间建立一个安全的连接，代理可以通过此连接发送数据。

此外，如果您正计划实施用户访问控制，则必须设置至您计划收集数据的每个 Microsoft Active Directory 服务器的连接，并配置用户感知参数。

有关详细信息，请参阅以下各节：

- 在防御中心上设置用户代理，第 2-3 页
- 设置 LDAP 连接以允许用户访问控制，第 2-3 页

在防御中心上设置用户代理

通过用户代理收集 LDAP 用户登录信息的第一步是配置每个防御中心，以允许来自用于连接 Active Directory 服务器的代理的连接。本章介绍在 5.x 版本的防御中心上配置授权代理连接的步骤。

要配置防御中心以连接到用户代理，请执行以下操作：

访问权限：管理员/发现管理员

步骤 1　选择 **Policies > Users**。

步骤 2　点击 **Add User Agent**。

步骤 3　在 **Name** 字段中，键入一个代理的描述性名称。

步骤 4　在 **Hostname or IP Address** 字段中键入代理将驻留的计算机的 IP 地址或主机名。必须使用 IPv4 地址；若使用 IPv6 地址，您将**无法**配置防御中心连接到用户代理。

注　您无法添加使用 IPv6 地址的用户代理或解析为 IPv6 地址的主机名。

步骤 5　点击 **Add User Agent**。

防御中心当前能够连接到所配置的主机上的用户代理。

步骤 6　您有以下选择：

- 如果需要执行用户控制，请继续设置 LDAP 连接以允许用户访问控制，第 2-3 页
- 如果不需要执行用户控制，请继续配置权限以连接到 Active Directory 服务器，第 2-4 页

设置 LDAP 连接以允许用户访问控制

如果需要执行用户控制 （即，撰写包含用户条件的访问控制规则），您必须配置并启用防御中心与贵公司的至少一个 Microsoft Active Directory 服务器之间的连接。此配置 （称为 *LDAP 连接*或*用户感知身份验证对象*）包含服务器相关的连接设置和身份验证过滤器设置。连接的用户和组访问控制参数指定了可在访问控制规则中使用的用户和组。

注　如果需要执行用户控制，**必须**使用 Microsoft Active Directory。系统通过在 Active Directory 服务器上运行的用户代理将用户与 IP 地址相关联，使得访问控制规则能够被触发。

有关设置带用户感知配置的 LDAP 连接的详细信息，请参阅《*FireSIGHT 系统用户指南*》。

配置权限以连接到 Active Directory 服务器

在计算机上准备好所有代理先决条件后，确认 Active Directory 安全日志已启用，使得 Active Directory 服务器能够将登录数据记录至这些日志。然后，配置用户权限和 Windows 安全权限，使得代理可以与 Active Directory 服务器通信并访问安全日志以获取登录数据，或者检索注销数据。

要确认 Active Directory 服务器正在记录登录数据，请执行以下操作：

步骤 1　在 Active Directory 服务器上，选择 **Start > All Programs > Tools > Event Viewer**。

步骤 2　选择 **Windows Logs > Security**。

如果已启用日志记录，则显示安全日志。如果已禁用记录，请参阅 http://technet.microsoft.com/en-us/library/cc779487(v=ws.10).aspx 查看有关启用安全日志记录的信息。

要允许代理与 Active Directory 服务器通信，请执行以下操作：

步骤 1　在 Active Directory 服务器上启用远程管理防火墙规则。您有以下选择：

- 如果 Active Directory 服务器运行 Windows Server 2003，请参阅 http://technet.microsoft.com/en-us/library/cc738900%28v=ws.10%29.aspx 以了解详细信息。
- 如果 Active Directory 服务器运行 Windows Server 2008 或 Windows Server 2012，请参阅 http://msdn.microsoft.com/en-us/library/aa822854%28VS.85%29.aspx 以了解详细信息。

要授权代理检索登录数据，请执行以下操作：

步骤 1　在待安装代理的计算机上创建一个用户。

注　当配置 Active Directory 服务器连接时，请使用这些凭证。有关详情，请参见配置用户代理与 Active Directory 服务器间的连接，第 2-9 页。

步骤 2　在 Active Directory 服务器上为用户启用 RPC。您有以下选择：

- 如果 Active Directory 服务器运行 Windows Server 2008 R2 或 Windows Server 2012，且用户不是管理员组的成员，则授予用户 DCOM 远程访问、远程启动和激活的权限。有关详细信息，请参阅 http://msdn.microsoft.com/en-us/library/Aa393266.aspx。
- 如果 Active Directory 服务器运行支持的其他 Microsoft Windows 版本，则已启用 RPC。

要授权代理检索注销数据，请执行以下操作：

步骤 1　向创建的用户授予管理员权限，确保该用户能够登录对 Active Directory 服务器进行身份验证的所有工作站。

要授权代理访问安全日志，请执行以下操作：

步骤 1　向创建的用户授予对 Active Directory 服务器上的 WMI 根/CIMV2 命名空间的完整许可权。有关详细信息，请参阅 http://technet.microsoft.com/en-us/library/cc787533%28v=WS.10%29.aspx。

继续执行启用空闲会话超时，第 2-5 页。

启用空闲会话超时

在配置权限以连接到 Active Directory 服务器之后，您可选择在组策略中启用空闲会话超时。这有助于防止代理检测和报告由于主机上的多个会话导致的无关登录。

终端服务允许多个用户同时登录到服务器。启用空闲会话超时有助于减少多个会话登录到同一服务器的情况。

远程桌面一次只允许一个用户远程登录工作站。但是，如果用户从远程桌面会话断开而不是注销，则会话保持活动状态。如果没有用户输入，活动会话最终会转为空闲状态。如果有另一用户使用远程桌面登录工作站，则两个会话同时运行。多个同时运行的会话可能导致代理报告无关的登录。启用空闲会话超后，这些会话将在定义的空闲超时时间之后终止，这有助于防止主机上的多个远程会话。

Citrix 会话的运作方式类似于远程桌面会话。多个 Citrix 用户会话可能在计算机上同时运行。启用空闲会话超时有助于防止主机上同时运行多个 Citrix 会话，减少无关的登录报告。

请注意，根据不同的会话超时配置，仍可能存在多个会话登录计算机的情况。

要启用终端服务会话超时，请执行以下操作：

步骤 1　更新空闲终端服务会话超时和已断开终端服务会话超时的组策略设置。您有以下选择：

- 如果 Active Directory 服务器运行 Windows Server 2008 或 Windows Server 2012，请参阅 http://technet.microsoft.com/en-us/library/cc754272(v=ws.10).aspx 以了解有关启用会话超时的详细信息。
- 如果 Active Directory 服务器运行 Windows Server 2003，请参阅 http://technet.microsoft.com/en-us/library/cc758177(v=ws.10).aspx 以了解有关启用会话超时的详细信息。

会话超时应设置为短于配置的注销检查频率，这样空闲和已断开会话才有可能在下次注销检查之前超时。如果有强制空闲会话或已断开会话超时，将配置的注销检查频率设置为大于会话超时。有关配置注销检查频率的详细信息，请参阅配置常规用户代理设置，第 2-16 页。

要启用远程桌面会话超时，请执行以下操作：

步骤 1　更新空闲远程会话超时和已断开会话超时的组策略设置。请参阅 http://technet.microsoft.com/en-us/library/ee791886%28v=ws.10%29.aspx 以了解有关启用会话超时的详细信息。

会话超时应设置为短于配置的注销检查频率，这样空闲和已断开会话才有可能在下次注销检查之前超时。如果有强制空闲会话或已断开会话超时，将配置的注销检查频率设置为大于会话超时。有关配置注销检查频率的详细信息，请参阅配置常规用户代理设置，第 2-16 页。

要启用 Citrix 会话超时，请执行以下操作：

步骤 1　请参阅 Citrix 的联机文档：http://support.citrix.com/。

继续执行在计算机上做好安装用户代理的准备，第 2-6 页。

在计算机上做好安装用户代理的准备

在配置防御中心以连接到将安装每个用户代理的 Windows 计算机之后，请在 Windows 计算机上设置以下先决条件：

- 计算机运行 Windows Vista、Windows 7、Windows 8、Windows Server 2003、Windows Server 2008 或 Windows Server 2012。计算机不必是一台 Active Directory 服务器。
- 计算机已安装 Microsoft .NET Framework 4.0 版本客户端配置文件和 Microsoft SQL Server Compact (SQL CE) 3.5 版本。可从 Microsoft 获取 .NET Framework 4.0 版本客户端配置文件可再分发软件包 (`dotNetFx40_Client_x86_x64.exe`)。可从 Microsoft 获取可执行文件形式的 SQL CE (`SSCERuntime-ENU.exe`)。

注　如果未安装 .NET Framework 和 SQL CE，当您打开代理可执行文件 (`Sourcefire_User_Agent_2.2-9_Setup.exe`) 时，计算机会提示您下载相应的文件。有关详细信息，请参阅安装用户代理，第 2-7 页。

- 计算机可通过 TCP/IP 访问待监控的 Active Directory 服务器，并且与 Active Directory 服务器使用相同版本的互联网协议。如果代理实时监控 Active Directory 服务器，计算机上的 TCP/IP 访问必须始终打开，以便检索登录数据。
- 计算机可通过 TCP/IP 访问您将报告数据的防御中心并且带有 一个 IPv4 地址。
- 计算机有一个 IPv6 地址（用于检测带有 IPv6 地址的主机上的注销）或一个 IPv4 地址（用于检测带有 IPv4 地址的主机上的注销）。
- 计算机没有已安装的旧版代理或 2.x 版本的代理。因为这些代理不会自动卸载，要卸载现有代理，请打开控制面板中的 **Add/Remove Programs**。

注意　如果已安装用户代理的早期版本，您必须完成数据库的备份以保留现有的配置设置。

继续执行备份用户代理配置，第 2-7 页。

备份用户代理配置

如果已安装用户代理的早期版本，安装用户代理的新版本后计算机会删除现有的配置。要保留这些配置设置，请在安装用户代理的新版本之前备份数据库。

注　如果已安装 2.2 版本或后续版本的用户代理，则不需要备份数据库。当安装用户代理的新版本时，计算机会自动导入配置设置。继续执行安装用户代理，第 2-7 页。

要保留现有配置设置，请执行以下操作：

步骤 1　在安装代理的计算机上，选择 **Start > Programs > Sourcefire > Configure User Agent**。

步骤 2　点击停止按钮 ( ) 以停止代理服务。

步骤 3　在安装代理的计算机上找到 `C:\SourcefireUserAgent.sdf`，并将该文件复制到本地。

步骤 4　导航到控制面板并打开 **Add/Remove Programs**，然后卸载 Sourcefire 用户代理。删除代理。

步骤 5　安装用户代理的最新版本。有关详细信息，请参阅安装用户代理，第 2-7 页。

步骤 6　在安装代理的计算机上，选择 **Start> Programs > Sourcefire > Configure User Agent**。

步骤 7　点击停止按钮 ( ) 以停止代理服务。

步骤 8　在已安装最新版本代理的计算机上找到 `C:\SourcefireUserAgent.sdf`。使用从代理先前版本进行的本地备份替换当前文件。

步骤 9　在已安装最新版本代理的计算机上，选择 **Start > Programs > Sourcefire > Configure User Agent**。

步骤 10　点击启动按钮 ( ) 以启动代理服务。代理服务启动。

继续执行配置用户代理，第 2-8 页。

安装用户代理

许可证：FireSIGHT

在配置权限以连接 Active Directory 服务器后，不管是否配置了空闲远程会话超时，都可安装代理。

注意　如果已安装有用户代理的早期版本，要保留现有配置设置，在安装前必须完成数据库的备份。有关详细信息，请参阅备份用户代理配置，第 2-7 页。

代理作为一项使用**本地系统**帐户的服务运行。如果运行代理的 Windows 计算机连接到网络，服务将继续轮询和发送用户数据，即使用户未登录计算机并处于活动状态。

注　请勿更改服务配置；帐户更改后，代理将无法正常工作。

对于每个代理，您可以配置与五台 Active Directory 服务器和五个防御中心的连接。在添加防御中心连接之前，请确保已将代理添加至防御中心配置。有关详细信息，请参阅准备连接到 4.x 版本的防御中心，第 2-2 页或准备连接到 5.x 版本的防御中心，第 2-2 页。

配置高可用性时，将两个防御中心都添加到代理，以将用户登录数据同时更新到主防御中心和辅助防御中心，从而使两个防御中心里的数据都为最新数据。

要安装用户代理，请执行以下操作：

访问权限：任意

步骤 1　从支持站点下载用户代理安装文件 (`Sourcefire_User_Agent_2.2-9_Setup.zip`)。

注　从支持站点直接下载安装文件，请勿通过邮件传输该文件。如果通过邮件传输安装文件，该文件可能会损坏。

步骤 2　将安装文件复制到待安装代理的计算机，然后解压缩该文件。

要求硬盘驱动器上有 3 MB 的可用空间以安装代理。思科建议您在硬盘驱动器上为代理的本地数据库分配 4 GB 的空间。

步骤 3　打开可执行文件 (`Sourcefire_User_Agent_2.2-9_Setup.exe`)。

提示　如果您使用的帐户不是管理员组的成员，无权在 Windows 计算机中安装新应用，则必须升级到拥有安装权限的管理员组的用户。要访问升级选项，右键点击 `Sourcefire_User_Agent_2.2-9_Setup.exe` 文件，然后选择 **Run As**。选择相应的用户并提供该用户的密码。

步骤 4　如果在安装代理的计算机上未安装 Microsoft .NET Framework 4.0 版本客户端配置文件和 SQL CE 3.5 版本，计算机会提示您下载相应的文件。下载并安装文件。

步骤 5　按照向导的提示安装代理。

步骤 6　要开始配置代理，请参阅配置用户代理，第 2-8 页。

配置用户代理

许可证：FireSIGHT

安装代理后进行配置，使代理从 Active Directory 服务器接收数据、将该信息报告给防御中心，对特定用户名和 IP 地址不进行报告，并将状态消息记录到本地事件日志或 Windows 应用程序日志。

要配置代理，请执行以下操作：

访问权限：任意

步骤 1　在安装代理的计算机上，选择 **Start > Programs > Sourcefire > Configure Sourcefire User Agent**。

下表对配置代理时可执行的操作及在何处进行配置进行了描述。

表 2-1　　用户代理配置操作

要.....	您可以.....
更改代理名称、更改注销检查频率、开始和停止服务以及设置调度优先级	选择 **General** 选项卡。有关详情，请参见配置常规用户代理设置，第 2-16 页。
添加、修改或删除 Active Directory 服务器，启用实时 Active Directory 服务器数据检索，以及修改 Active Directory 服务器轮询间隔和最大轮询时间	选择 **Active Directory Servers** 选项卡。有关详情，请参见配置用户代理与 Active Directory 服务器间的连接，第 2-9 页。
添加或删除防御中心	选择 **Sourcefire DCs** 选项卡。有关详情，请参见配置用户代理防御中心连接，第 2-12 页。
添加、修改或删除报告排除的用户名	选择 **Excluded Usernames** 选项卡。有关详情，请参见配置用户代理排除用户名设置，第 2-13 页。
添加、修改或删除报告排除的 IP 地址	选择 **Excluded Addresses** 选项卡。有关详情，请参见配置用户代理排除地址设置，第 2-14 页。
查看、导出和清除事件日志，记录到 Windows 应用程序日志以及修改消息的保存时间	选择 **Logs** 选项卡。有关详情，请参见配置用户代理日志记录设置，第 2-14 页。
按照技术支持的指示执行故障排除和维护任务	选择 **Logs** 选项卡，启用 **Show Debug Messages in Log**，然后选择 **Maintenance** 选项卡。有关详情，请参见配置用户代理维护设置，第 2-17 页。
保存对代理设置的更改	点击 **Save**。当更改未保存时，在 **Save** 下会显示提示消息。
关闭代理，不保存对代理设置的更改	点击 **Cancel**。

配置用户代理与 Active Directory 服务器间的连接

许可证：FireSIGHT

您可以添加连接，将代理连接到最多五台 Active Directory 服务器，并配置：

- 代理是实时检索登录和注销数据，还是定期轮询 Active Directory 服务器检索数据
- 代理轮询用户活动数据的频率或连接失败时尝试建立或重新建立与 Active Directory 服务器的实时连接的重试次数
- 代理向 Active Directory 服务器报告的登录该服务器的 IP 地址
- 当代理建立或重新建立与 Active Directory 服务器的连接时检索的登录和注销数据量

当代理配置为实时检索数据且实时监控不可用时，代理会改为尝试轮询 Active Directory 服务器检索数据，直到实时监控变为可用。

提示　如果用户代理检索到大量用户活动，思科建议配置轮询而非实时数据检索。在存在大量活动的环境中，请配置 1 分钟的轮询间隔和不超过 10 分钟的最大轮询时间。

请注意，如果 Active Directory 运行 Windows Server 2003，则代理不能被配置为监控该服务器。实时监控要求 Active Directory 服务器运行 Windows Server 2008 或更高版本。

通过代理可查看在选择选项卡时当前 Active Directory 服务器的轮询状态、向代理报告的最后一次登录以及代理最后一次轮询 Active Directory 服务器的时间。还可以查看代理是否正在实时轮询 Active Directory 服务器以及选择选项卡时的实时数据检索状态。请参阅下表以了解有关服务器状态的详细信息。

表 2-2　Active Directory 服务器状态

Active Directory 服务器状态	轮询可用性	实时可用性
数	服务器可提供轮询。	服务器可提供实时数据检索。
unavailable	服务器不提供轮询。	服务器不提供实时数据检索，或者服务器配置为轮询。
pending	服务器配置已添加，但尚未保存。	服务器配置已添加，但尚未保存。
unknown	代理已启动且状态尚不可用，或代理尚未检查 Active Directory 服务器。	代理已启动且状态尚不可用，或代理尚未检查 Active Directory 服务器。

注　不可将多个用户代理连接到同一 Active Directory 服务器，由于每个代理都会检测到其他代理的连接，这些代理将报告无关的登录。如果多个用户代理被连接到同一 Active Directory 服务器，请配置各个代理，排除运行轮询同一 Active Directory 服务器的代理的所有其他主机的 IP 地址，以及该代理用于登录的用户名。有关详细信息，请参阅配置用户代理排除地址设置，第 2-14 页。

要配置 Active Directory 服务器连接，请执行以下操作：

访问权限：任意

步骤 1　选择 **Active Directory Servers** 选项卡。

步骤 2　此时您有两种选择：

- 要将一个新的连接添加至服务器，请点击 **Add**。
- 要修改现有连接，双击服务器名称。

提示　要删除现有连接，选择服务器名称并点击 **Remove**。

步骤 3　在 **Server Name/IP Address** 字段中，键入 Active Directory 服务器可充分识别的服务器名或 IP 地址。如果要检测 Active Directory 服务器上的登录，请键入 IP 地址。

注　如果代理安装在 Active Directory 服务器上，要添加安装代理的服务器，服务器名称请键入 `localhost`。可以选择添加用户名和密码。如果忽略此信息，将无法检测到该 Active Directory 服务器上的注销。无论您是否输入用户名和密码，都可轮询服务器。

步骤 4　键入一个有权限查询 Active Directory 服务器上的用户登录和注销数据的用户名和密码。要使用户通过代理进行身份验证，请键入一个完全限定的用户名。

默认情况下，用来登录安装代理的计算机的帐户的域会自动填充 **Domain** 字段。

注　如果用户密码包含 65 个或以上字符，则无法配置新的服务器连接。要恢复此功能，请将密码缩短。

步骤 5　在 Domain 字段中输入 Active Directory 服务器充当域的域。

步骤 6　要检测 Active Directory 服务器上的登录，请从 **Local Login IP Address** 字段中选择 IP 地址。代理使用与 **Server Name/IP Address** 字段中指定的服务器相关联的所有 IP 地址来自动填充此字段。

如果 **Server Name/IP Address** 字段为空或包含 `localhost`，代理则使用与本地主机相关联的所有 IP 地址来填充此字段。

步骤 7　选择 **Process real-time events**，使得用户代理能从该 Active Directory 服务器中实时检索登录事件。

步骤 8　点击**添加**。

在 Active Directory 服务器列表中显示了服务器连接定义。如果已配置不止一个服务器连接，可以通过点击相应列标题按 **Host**、**Last Reported**、**Polling Status**、**Last Polled**、**Real-time Status** 或 **Real-time** 排序。

注　如果代理在配置时无法连接到 Active Directory 服务器，则无法添加此服务器。检查确认代理可通过 TCP/IP 访问服务器，使用的凭证可以连接，以及已正确配置与 Active Directory 服务器的连接。有关详情，请参见配置权限以连接到 Active Directory 服务器，第 2-4 页。

步骤 9　或者，若要更改代理自动轮询 Active Directory 服务器检索用户登录数据的间隔，请从 **Active Directory Server Polling Interval** 下拉列表中选择时间。

设置保存后，下一次轮询会在选定的分钟数后进行，并按照该间隔重复进行。如果轮询花费的时间比选定间隔长，下一次轮询会在此轮询结束后的下一个间隔启动。如果对 Active Directory 服务器启用了实时数据检索，并且代理与该服务器的连接失败，代理会继续尝试轮询，直到接收到回应并且实时数据检索变为可用。一旦连接已建立，实时数据检索随即恢复。

步骤 10　或者，若要更改代理首次建立或重新建立与 Active Directory 服务器的连接以轮询用户登录数据时轮询的最大时间范围，请从 **Active Directory Server Max Poll Length** 下拉列表中选择一个时间。

注　在 **Active Directory Server Max Poll Length** 下拉列表中保存的值不能小于从 **Active Directory Server Polling Interval** 下拉列表中选择的值。代理不允许保存使得在每次轮询中都将跳过用户活动数据的配置。

步骤 11　要保存配置更改并应用到代理，请点击 **Save**。

步骤 12　您有以下选择：

- 要添加或删除防御中心连接，选择 **Sourcefire DCs** 选项卡。有关详细信息，请参阅配置用户代理防御中心连接，第 2-12 页。

  必须将至少一个防御中心添加到代理，以报告用户登录和注销数据。
- 要配置代理，您可以执行表 2-1，第 2-9 页中所述的任何一种操作。

配置用户代理防御中心连接

许可证：FireSIGHT

可添加连接，将代理连接到最多五个防御中心。通过代理可查看选择选项卡时的防御中心状态（当第一次启动代理时为 `available`、`unavailable` 或 `unknown`）以及代理报告的上一次登录。在添加连接之前，请确保已将代理添加至防御中心配置。有关详细信息，请参阅准备连接到 4.x 版本的防御中心，第 2-2 页或准备连接到 5.x 版本的防御中心，第 2-2 页。

配置高可用性时，将两个 防御中心都添加到代理，以将用户登录和注销数据同时更新到主防御中心和辅助防御中心，从而使两个防御中心里的数据都为最新数据。

要配置防御中心连接，请执行以下操作：

访问权限：任意

步骤 1　选择 **Sourcefire DCs** 选项卡。

步骤 2　点击**添加**。

步骤 3　键入待添加的防御中心的主机名或 IP 地址。

步骤 4　点击**添加**。

防御中心连接配置添加成功。不可多次添加同一主机名或 IP 地址。不可同时通过使用主机名和 IP 地址添加防御中心。如果防御中心为多宿主，不可使用不同的 IP 地址多次添加该防御中心。

如果配置了多个防御中心连接，可以通过点击相应的列标题按 **Host**、 **Status** 或 **Last Reported** 进行排序。

注　如果代理在配置时无法连接到防御中心，则代理无法添加该防御中心。检查确认代理能够通过 TCP/IP 访问防御中心。

步骤 5　要保存配置更改并应用到代理，请点击 **Save**。更新设置已应用到代理。

步骤 6　您有以下选择：

- 或者，要添加或删除 “排除用户名”列表中的用户名，请选择 **Excluded Usernames** 选项卡。有关详细信息，请参阅配置用户代理排除用户名设置，第 2-13 页。
- 或者，要添加或删除 “排除 IP 地址”列表中的 IP 地址，请选择 **Excluded Addresses** 选项卡。有关详细信息，请参阅配置用户代理排除地址设置，第 2-14 页。
- 或者，要查看日志消息和配置日志记录，请选择 **Logs** 选项卡。有关详细信息，请参阅配置用户代理日志记录设置，第 2-14 页。
- 或者，要配置常规代理设置，请选择 **General** 选项卡。有关详细信息，请参阅配置常规用户代理设置，第 2-16 页。
- 要配置代理，您可以执行表 2-1，第 2-9 页中所述的任何一种操作。

配置用户代理排除用户名设置

许可证：FireSIGHT

可以定义最多 500 个在轮询登录或注销事件时要排除的用户名。如果代理检索到由排除用户名执行的登录或注销事件，代理不会将此事件报告给防御中心。在排除之前报告的登录和注销事件不受影响。如果从排除用户名列表中删除用户名，该用户名未来的登录和注销事件将报告给防御中心。

可以选择是排除用户从所有域执行的所有登录和注销，还是仅排除从特定的域执行的登录和注销。还可以导出和导入用户名和域的列表，这些列表保存在逗号分隔值文件中。请注意，如果排除已报告给防御中心的用户，则永远不会取消此用户到主机的映射，除非从数据库中删除该主机。

要配置排除用户名，请执行以下操作：

访问权限：任意

步骤 1　选择 **Excluded Usernames** 选项卡。

步骤 2　在下一个可用行的 **Username** 列中，键入待排除的用户名。

排除的用户名不能含有美元符号字符 ($) 或引号字符 (")。

步骤 3　或者，在 **Domain** 列中键入与该用户名相关联的域。每行只能定义一个域。如果不指定域，则会排除每个域中的该用户名。

步骤 4　重复第 2 步和第 3 步，以添加更多用户名称。如果已配置多个排除用户名，可通过点击相应的列标题按 **Username** 或 **Domain** 排序。

步骤 5　要删除一行，您有以下选择：

- 突出显示行，然后按 Delete 键。
- 将光标置于用户名末尾并按 Backspace 键，直到将其删除。

该行删除成功。

要删除多行，按住 Ctrl 键并点击选择多行，然后按 Delete 键。

步骤 6　要将用户名和域的列表导出到一个逗号分隔值文件，请点击 **Export List**。选择保存文件的文件路径。

文件将被保存。默认情况下，文件名为 `Sourcefire_user_agent_excluded_users.csv`。

步骤 7　要从一个逗号分隔值文件导入用户名和域的列表，请点击 **Import List**。选择要上传的文件。

现有用户名会被清除，并且将加载文件中的用户名。包含重复用户名的文件将无法上传。如果文件中有任何语法错误，则无法上传文件。

逗号隔开值文件中的条目必须为以下格式：

"*用户名*","*域*"

域值是可选的，但是必须使用引号作为占位符。

步骤 8　点击 **Save**，保存配置更改并应用到代理。

更新设置已应用到代理。

步骤 9　您有以下选择：

- 要添加或删除 “排除 IP 地址”列表中的 IP 地址，请选择 **Excluded Addresses** 选项卡。有关详细信息，请参阅配置用户代理排除地址设置，第 2-14 页。
- 要配置代理，您可以执行表 2-1，第 2-9 页中所述的任何一种操作。

配置用户代理排除地址设置

许可证：FireSIGHT

可以定义最多 100 个在轮询登录事件时要排除的 IPv4 或 IPv6 地址。如果检索到包含排除 IP 地址的登录或注销事件，代理不会将此事件报告给防御中心。在排除之前报告的来自该 IP 地址的登录和注销事件不受影响。如果您从故障排除地址列表中删除一个 IP 地址，该地址未来的登录和注销事件将报告给防御中心。

要配置排除 IP 地址，请执行以下操作：

访问权限：任意

步骤 1　选择 **Excluded Addresses** 选项卡。

步骤 2　在下一个可用行的 **Address** 列中，键入要排除的 IP 地址。重复此步骤以添加更多 IP 地址。如果配置了不止一个排除 IP 地址，可通过点击相应的列标题按 **Address** 排序。

如果输入的 IP 地址无效，行标题中会显示感叹号图标 ( )。在修正此无效地址之前，无法输入另一地址。

步骤 3　要删除 IP 地址，请突出显示该行，然后按 Delete 键。

该 IP 地址即被删除。要删除多行，按住 Ctrl 键并点击选择多行，然后按 Delete 键。

步骤 4　要将 IP 地址列表导出到一个逗号分隔值文件，点击 **Export List**。选择保存文件的文件路径。

文件将被保存。默认情况下，文件名为 `Sourcefire_user_agent_excluded_addresses.csv`。

步骤 5　要从一个逗号分隔值文件导入 IP 地址列表，点击 **Import List**。选择要上传的文件。

现有 IP 地址会被清除，并且将加载文件中的 IP 地址。包含重复 IP 地址的文件将无法上传。如果文件中有任何语法错误，则无法上传文件。

步骤 6　点击 **Save**，保存配置更改并应用到代理。

更新设置已应用到代理。

步骤 7　您有以下选择：

- 要查看日志消息和配置日志记录，请选择 **Logs** 选项卡。有关详细信息，请参阅配置用户代理日志记录设置，第 2-14 页。
- 要配置代理，您可以执行表 2-1，第 2-9 页中所述的任何一种操作。

配置用户代理日志记录设置

许可证：FireSIGHT

在 **Logs** 选项卡中可查看最多 250 条由代理记录的状态消息。在发生下列事件时，代理将状态消息记录到本地事件日志：

- 代理成功轮询 Active Directory 服务器上的数据
- 代理无法连接到 Active Directory 服务器
- 代理无法从 Active Directory 服务器检索数据
- 代理已成功连接到思科设备
- 代理无法连接到思科设备

代理记录的每条消息都带有时间戳和严重级别。下表按照严重性递增的顺序说明可能的严重级别。

表 2-3　用户代理日志严重级别

功率水平	颜色	说明
调试	灰色	记录此事件是为了用于调试。 默认情况下这些消息不会显示。
信息	green	事件与正常代理操作一致。
警告	yellow	事件发生于意料之外，但不一定会影响代理的正常运行。
错误	红色	事件发生于意料之外，并且会影响代理的正常运行。

除了记录到本地事件日志，代理还可以将状态消息记录到 Windows 应用程序日志。代理也可以将本地事件日志内容导出到逗号分隔值文件。

可以配置是否存储状态消息、存储时间以及清除所有状态消息的事件日志。还可以配置维护选项（例如，查看调试状态消息）和访问 **Maintenance** 选项。

注　调试状态消息会在事件日志中存储七天。配置状态消息存储时间和清除事件日志不会影响调试状态消息存储。

要配置用户代理日志记录设置，请执行以下操作：

访问权限：任意

步骤 1　选择 **Logs** 选项卡。

步骤 2　如果技术支持指示您执行此操作，请选择 **Show Debug Messages in Log** 查看事件日志中的调试状态消息并启用 **Maintenance** 选项卡。

调试状态消息显示在 **Logs** 选项卡中。 **Maintenance** 选项卡可用。

注　仅当技术支持指示您执行此操作时，才选择此选项。

步骤 3　选择 **Log Messages to Windows Application Log** 以将非调试状态消息同时记录到 Windows 应用程序日志和本地事件日志。

要查看 Windows 应用程序日志，请打开 Windows 事件查看器。

步骤 4　从 **Message Cache Size** 下拉列表中选择一个时间段，以配置状态消息在从本地事件日志中被自动删除之前的保存时间。

一旦记录到本地事件日志中，状态消息在 **Message Cache Size** 下拉列表中选定的时间段内会被保存，时间段过后则被删除。

注　**Message Cache Size** 设置仅影响本地事件日志，即使选择 **Log Messages to Windows Application Log**，也不影响 Windows 应用程序日志。

步骤 5　点击 Refresh 查看上次刷新以来记录的新状态消息。

如果自上次刷新后记录了新的状态消息，将显示注释提示有新的状态消息。如果因刷新而显示的消息超过 250 条，最早的状态消息将从 **Logs** 选项卡中删除。要查看超过 250 条消息，请导出日志。有关详细信息，请参阅步骤 6。

步骤 6　点击 **Export Logs** 将本地事件日志内容导出到逗号分隔值文件。

该逗号分隔值文件包含所有事件日志状态消息和调试消息。

步骤 7　点击 **Clear Event Log** 从本地事件日志中删除所有非调试状态消息。

除说明删除了消息的代理的状态消息之外，本地事件被清空。

步骤 8　要保存配置更改并应用到代理，请点击 **Save**。

更新设置已应用到代理。

步骤 9　您有以下选择：

- 要配置常规代理设置，请选择 **General** 选项卡。有关详细信息，请参阅配置常规用户代理设置，第 2-16 页。
- 要配置代理，您可以执行表 2-1，第 2-9 页中所述的任何一种操作。

配置常规用户代理设置

许可证：FireSIGHT

General 选项卡包含用户代理基本配置。可以更改代理报告登录数据时报告给防御中心的代理名称。还可以开始和停止代理服务、更改注销检查频率和查看当前的服务状态。

要配置常规用户代理设置，请执行以下操作：

访问权限：任意

步骤 1　在安装代理的计算机上，选择 **Start > Programs > Sourcefire > Configure User Agent**。

步骤 2　点击启动按钮 ( ) 以启动代理服务。

代理服务启动。

步骤 3　点击停止按钮 ( ) 以停止代理服务。

代理服务停止。

步骤 4　或者，修改代理的 **Agent Name** （默认为 `SFADUA`）。可以输入字母、数字、下划线 (_) 和破折号 (-)。

步骤 5　或者，在 5.2 版本及更高版本中，从 **Logout Check Frequency** 下拉列表中选择一个时间段，更改代理检查注销数据的频率。选择 `0` 禁用检查注销数据。

步骤 6　或者，从 **Priority** 下拉列表中选择一个级别，更改代理调度优先级。仅当代理监控并检索大量用户活动时，才选择 `High`。

步骤 7　要保存设置，请点击 **Save**。

更新设置已应用到代理。

步骤 8　要配置代理，您可以执行表 2-1，第 2-9 页中所述的任何一种操作。

配置用户代理维护设置

许可证：FireSIGHT

除配置设置以外，代理还会将用户到 IP 映射信息、本地事件日志和报告状态信息存储在 SQL CE 数据库中。代理 Maintenance 选项卡允许为了维护用户代理清除部分数据库。可以清除缓存的用户到 IP 映射信息和本地事件日志信息。还可以清除报告状态缓存，此操作会导致对已配置的 Active Directory 服务器强制进行手动轮询。

注意　除非技术支持指示您操作，否则，请**勿**更改 Maintenance 选项卡的任何设置。

要配置用户代理维护设置，请执行以下操作：

访问权限：任意

步骤 1　选择 **Logs** 选项卡。

步骤 2　选择 **Show Debug Messages in Log** 以启用 **Maintenance** 选项卡。

步骤 3　选择 **Maintenance** 选项卡。

步骤 4　点击 **Clear user mapping data cache** 以清除所有存储的用户到 IP 映射数据。

代理会删除本地代理数据库中存储的所有用户到 IP 映射数据。清除本地代理数据库不会影响在防御中心数据库中存储的用户到 IP 映射数据。

步骤 5　点击 **Clear logon event log cache** 清除所有存储的登录事件数据。

代理会删除本地事件日志中存储的所有登录事件数据。

步骤 6　点击 **Clear reporting state cache** 清除与上次代理向已配置的防御中心报告登录和注销信息相关的数据。

代理会删除与上次代理向已配置的防御中心报告登录和注销信息相关的所有信息。在下一次轮询间隔开始时，代理会手动轮询所有已配置的 Active Directory 服务器，检索在 **Active Directory Server Max Poll Length** 字段中定义的时间范围内的信息。有关详细信息，请参阅配置用户代理与 Active Directory 服务器间的连接，第 2-9 页。

步骤 7　从 **Debug Log Level** 下拉列表中选择日志记录粒度等级，配置所记录的调试消息的详细程度。

步骤 8　要配置代理，您可以执行表 2-1，第 2-9 页中所述的任何一种操作。