



## Cisco ISE 和 WSA 集成指南

[Cisco ISE 和 WSA 集成](#) 2

[Cisco ISE 和 WSA 集成概述](#) 2

[ISE-WSA 部署](#) 2

[支持的 ISE 和 WSA 版本](#) 3

[Cisco ISE 和 WSA 集成工作流程](#) 3

[使用 WSA 报告查看用户状态](#) 16

[使用日志文件对 ISE-WSA 集成问题进行故障排除](#) 16

[对 ISE-WSA 集成问题进行故障排除 - ISE 服务器连接](#) 18

[与 ISE-WSA 集成有关的 SMA 的概述](#) 19

Revised: November 9, 2015,

# Cisco ISE 和 WSA 集成

## Cisco ISE 和 WSA 集成概述

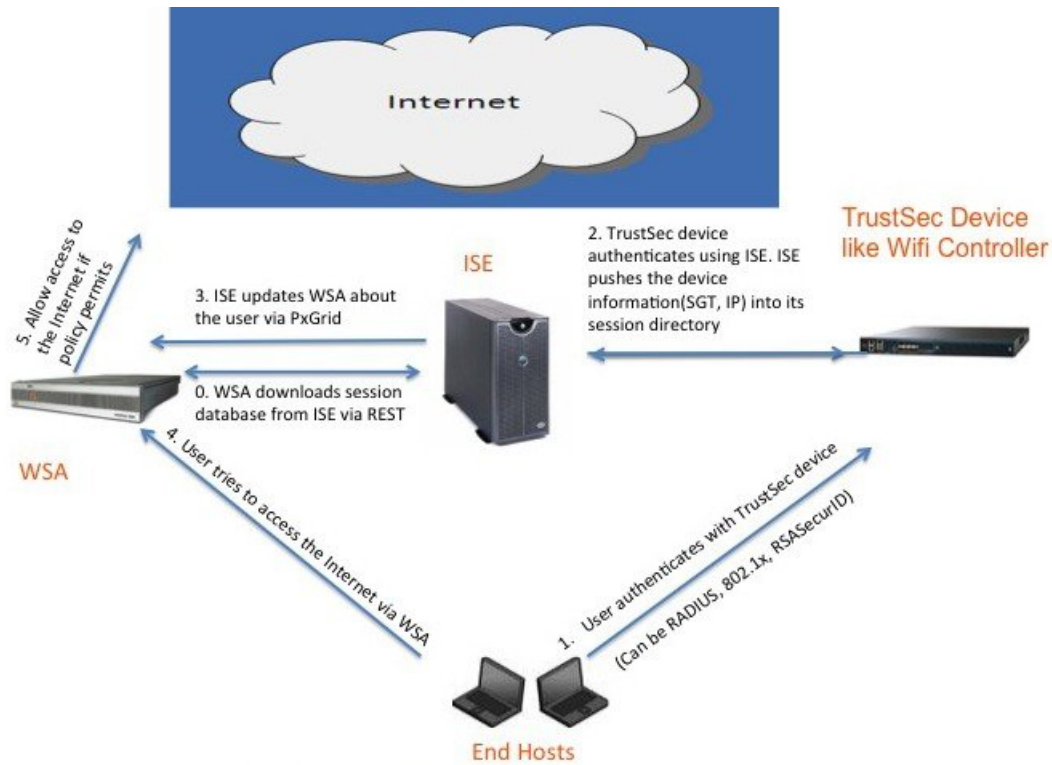
集成思科身份服务引擎 (ISE) 和 Web 安全设备 (WSA) 使 WSA 可以使用 ISE 提供的大量功能来识别终端并应用适当的访问策略，其中最重要的是 TrustSec 安全组标记 (SGT) 功能。使用 TrustSec SGT 功能，您可以将用户分类为不同的身份组。例如，属于安全组 SGT10 的用户只能访问某些社交网站。WSA 中的访问策略是使用 ISE 向用户会话分配的 SGT 标记创建而成的。

WSA 不支持 802.1X 等身份验证方法。通过将 WSA 与 ISE 集成，您可以使用更安全的 802.1X 身份验证方法通过 ISE 对 WSA 用户进行身份验证。利用 Cisco pxGrid 功能可以向 WSA 分享来自 Cisco ISE 的基于情景的信息，从而对用户进行授权以及应用相应策略。

## ISE-WSA 部署

通过集成 ISE 和 WSA，您可以根据用户的 IP 地址识别用户，因为 Cisco WSA 可从 Cisco ISE 获取 IP-用户映射。为了降低延迟和性能影响，建议在部署过程中在 Cisco ISE 和 WSA 之间保持最小距离。

下图描述了 Cisco ISE-WSA 集成工作流程。



## 支持的 ISE 和 WSA 版本

- Cisco ISE 版本 1.3
- Cisco WSA 版本 8.7.0 和更高版本

## Cisco ISE 和 WSA 集成工作流程

将 Cisco ISE 与 WSA 集成应遵循以下步骤：

### 过程

- 
- 步骤 1 为 WSA 客户端创建 SGT。
  - 步骤 2 设置 WSA。
  - 步骤 3 在 WSA 上配置 ISE 功能。
  - 步骤 4 为 WSA 客户端创建身份配置文件。
  - 步骤 5 为 WSA 客户端创建访问策略。
-

## 为 WSA 客户端创建 SGT

要开始集成，您需要为用户创建一个新身份组（例如 IDGroup3），然后将该身份组关联到一个 SGT（例如 SGTGroup3）。最后，您需要创建一个策略集，该策略集对属于您之前创建的身份组的用户使用 IEE 802.1X 身份验证。

### 开始之前

- 确保从 ISE 服务器删除所有现有 WSA 客户端（**管理 (Administration) > pxGrid 服务 (pxGrid Services) > 客户端 (Clients)**）。
- 确保在 ISE 中填充 WSA 客户端 IP 地址，以处理来自 WSA 的请求。
- 确保已启用 pxGrid 服务。确认 pxGrid 服务页面上显示“Connected to pxGrid”消息。（**管理 (Administration) > pxGrid 服务 (pxGrid Services)**）
- 确保您已生成 CA 签名的证书。
- 确保只要在 ISE 服务器上更改了证书，就重新启动 ISE 服务器。
- 选择**管理 (Administration) > 证书 (Certificates) > 受信任证书 (Trusted Certificates) > 导入 (Import)**，导入 pxGrid 证书、ISE 服务器管理员证书以及 WSA 证书和密钥，以便在 ISE 和 WSA 之间实现双向通信。
- 在角色 (Personas) 部分，选择**管理 (Administration) > 系统 (System) > 部署 (Deployment) > 常规设置 (General Settings)** 页面，然后选中 pxGrid 复选框，以便 ISE 和 WSA 之间进行通信。
- 选择**管理 (Administration) > pxGrid 服务 (pxGrid Services)**，然后选择启用自动注册 (**Enable Auto-Registration**) 选项。如果已禁用“自动注册” (Auto-Registration) 选项，当 WSA pxGrid 客户端尝试连接 ISE 上的 pxGrid 服务器时，ISE 服务器管理员必须手动允许 WSA 客户端注册。
- 选择**管理 (Administration) > 证书 (Certificates) > 受信任证书 (Trusted Certificates) > 编辑 (Edit)** 页面来编辑 WSA 证书。选中**使用 (Usage)** 部分中信任范围 (**Trusted For**) 选项下的所有复选框。
- 选择**管理 (Administration) > 系统 (System) > 设置 (Settings) > 协议 (Protocols) > ERS 设置 (ERS Settings)** 页面，然后在主管理节点 **ERS 设置 (ERS Setting for Primary Administration Node)** 部分启用启用读/写 ERS (**Enable ERS for Read/Write**)，从而使 REST 服务器可以与 WSA 通信。

### 过程

- 
- 步骤 1** 选择**管理 (Administration) > 身份管理 (Identity Management) > 组 (Groups) > 添加 (Add)**，创建 WSA 用户身份组。

User Identity Groups > New User Identity Group

**Identity Group**

\* Name

Description

User Identity Groups

Name	Description
<input type="checkbox"/> ALL_ACCOUNTS (default)	Default ALL_ACCOUNTS (default) User Group
<input type="checkbox"/> Employee	Default Employee User Group
<input type="checkbox"/> GROUP_ACCOUNTS (default)	Default GROUP_ACCOUNTS (default) User Group
<input type="checkbox"/> GuestType_Contractor (default)	Identity group mirroring the guest type
<input type="checkbox"/> GuestType_Daily (default)	Identity group mirroring the guest type
<input type="checkbox"/> GuestType_Weekly (default)	Identity group mirroring the guest type
<input type="checkbox"/> IDgroup10	
<input type="checkbox"/> IDgroup11	IDgroup11
<input type="checkbox"/> IDgroup12	IDgroup12
<input type="checkbox"/> IDgroup13	IDgroup13
<input type="checkbox"/> IDgroup14	IDgroup14
<input type="checkbox"/> IDgroup2	
<input type="checkbox"/> IDgroup3	
<input type="checkbox"/> IDgroup4	
<input type="checkbox"/> IDgroup5	
<input type="checkbox"/> IDgroup6	
<input type="checkbox"/> IDgroup7	
<input type="checkbox"/> IDgroup8	
<input type="checkbox"/> IDgroup9	
<input type="checkbox"/> OWN_ACCOUNTS (default)	Default OWN_ACCOUNTS (default) User Group

**步骤 2** 选择策略 (Policy) > 策略元素 (Policy Elements) > 结果 (Results) > TrustSec > 安全组 (Security Groups) > 添加 (Add), 在“安全组” (Security Groups) 页面定义所需的与 WSA 相关的 SGT。

Security Groups List > SGTgroup3

Security Groups

\* Name  Generation Id: 0

Description

Security Group Tag (Dec / Hex): 4/0004

Security Groups

For Policy Export go to [Administration > System > Backup & Restore > Policy Export Page](#)

<input type="button" value="Edit"/> <input type="button" value="Add"/> <input type="button" value="Import"/> <input type="button" value="Export"/> <input type="button" value="Delete"/> <input type="button" value="Push"/>			
<input type="checkbox"/>	Name ▲	SGT (Dec / Hex)	Description
<input type="checkbox"/>	RamaSGTgrou...	2/0002	RamaSGTgroup-IPs
<input type="checkbox"/>	RamaSGTgrou...	3/0003	
<input type="checkbox"/>	SGTgroup10	11/000B	
<input type="checkbox"/>	SGTgroup11	12/000C	SGTgroup11
<input type="checkbox"/>	SGTgroup12	13/000D	SGTgroup12
<input type="checkbox"/>	SGTgroup13	14/000E	SGTgroup13
<input type="checkbox"/>	SGTgroup14	15/000F	SGTgroup14
<input type="checkbox"/>	SGTgroup15	16/0010	SGTgroup15
<input type="checkbox"/>	SGTgroup18	17/0011	
<input type="checkbox"/>	SGTGroup19	18/0012	SGTGroup19
<input type="checkbox"/>	<b>SGTgroup3</b>	4/0004	
<input type="checkbox"/>	SGTgroup4	5/0005	

步骤 3 选择管理 (Administration) > 身份管理 (Identity Management) > 身份 (Identities) > 用户 (Users)。

步骤 4 点击添加 (Add)，创建网络访问用户。

▼ Network Access User

\* Name

Status  Enabled ▼

Email

▼ Password

\* Password  Need help with password policy ? ⓘ

\* Re-Enter Password

▼ User Information

First Name




Last Name

▼ Account Options

Description

Change password on next login

▼ User Groups



## Network Access Users

Edit Add Change Status Import Export Delete Duplicate							
	Status	Name	Description	First Name	Last Name	Email Address	User Identity Gro...
<input type="checkbox"/>	Enabled	linh					Employee
<input type="checkbox"/>	Enabled	user1		user1	user1		Employee
<input type="checkbox"/>	Enabled	user10		user10	user10		IDgroup10
<input type="checkbox"/>	Enabled	user100		user100	user100		IDgroup10
<input type="checkbox"/>	Enabled	user101		user101	user101		Employee
<input type="checkbox"/>	Enabled	user102		user	102		Employee
<input type="checkbox"/>	Enabled	user103		user	103		Employee
<input type="checkbox"/>	Enabled	user11		user11	user11		IDgroup11
<input type="checkbox"/>	Enabled	user111		user111	user111		IDgroup11
<input type="checkbox"/>	Enabled	user12		user12	user12		IDgroup12
<input type="checkbox"/>	Enabled	user122		user122	user122		IDgroup12
<input type="checkbox"/>	Enabled	user13		user13	user13		IDgroup13
<input type="checkbox"/>	Enabled	user133		user133	user133		IDgroup13
<input type="checkbox"/>	Enabled	user14		user14	user14		IDgroup14
<input type="checkbox"/>	Enabled	user144		user144	user144		IDgroup14
<input type="checkbox"/>	Enabled	user15		user15	user15		GuestType_Contr...
<input type="checkbox"/>	Enabled	user155		user155	user155		GuestType_Contr...
<input type="checkbox"/>	Enabled	user18		user18	user18		Employee
<input type="checkbox"/>	Enabled	user19		user19	user19		Employee
<input type="checkbox"/>	Enabled	user2		user2	user2		IDgroup2
<input type="checkbox"/>	Enabled	user22		user22	user22		IDgroup2
<input type="checkbox"/>	Enabled	user3		user3	user3		IDgroup3
<input type="checkbox"/>	Enabled	user33		user33	user33		IDgroup3
<input type="checkbox"/>	Enabled	user4		user4	user4		IDgroup4
<input type="checkbox"/>	Enabled	user44		user44	user44		IDgroup4

用户会分配至不同的 ID 组。

**步骤 5** 选择策略 (Policy) > 策略集 (Policy Sets) > 无线 WGA (WirelessWGA) > 授权策略 (Authorization Policy), 创建适用于身份和 SGT 组的规则。



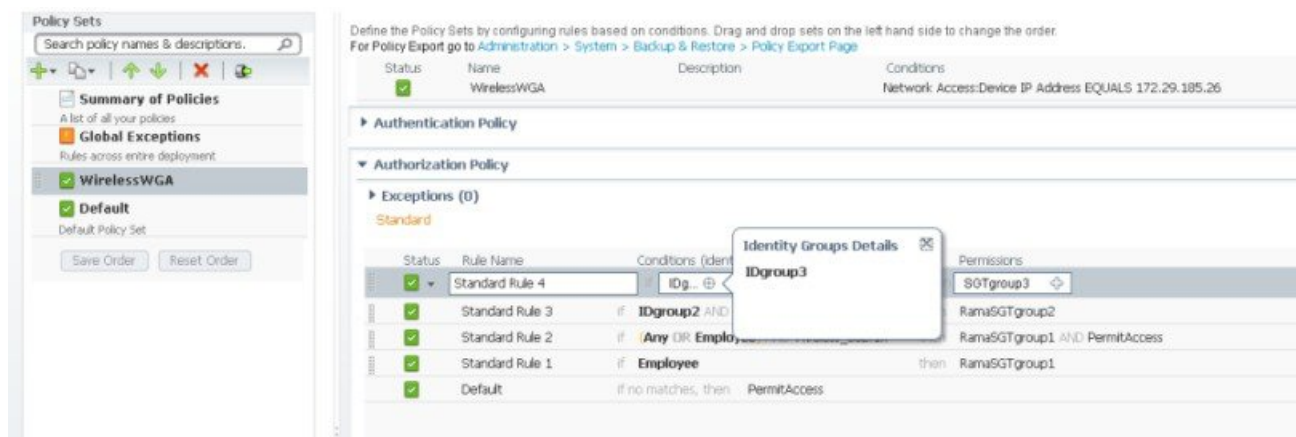
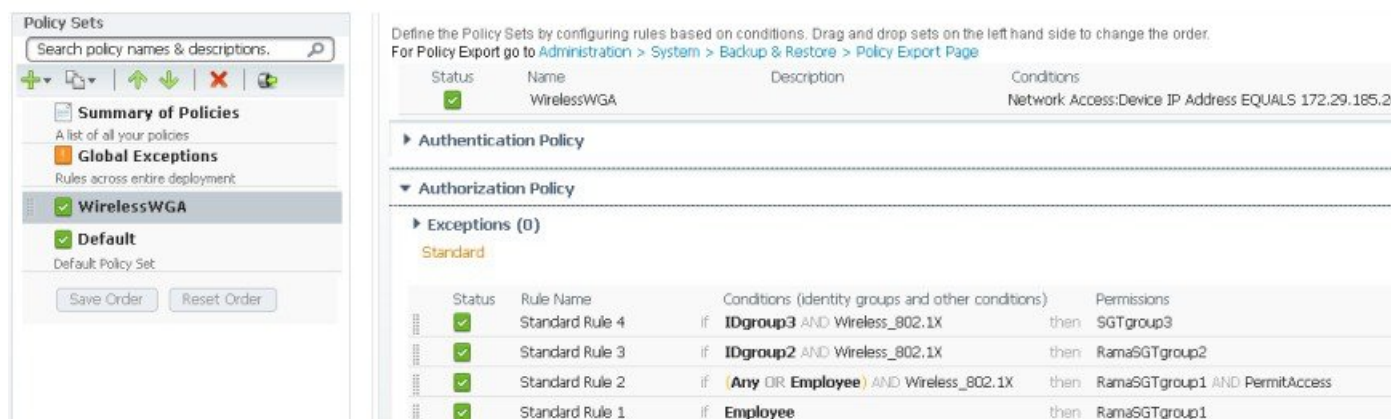


图 1:



接下来的操作

您应该为 ISE-WSA 集成配置 WSA。

## 设置 WSA

开始之前

- 将 WSA 设备连接至网络和设备。
- 完成“系统设置向导” (System Setup Wizard) 工作表。
- 如果您计划在虚拟设备上运行“系统设置向导” (System Setup Wizard)，请使用 loadlicense 命令加载虚拟设备许可证。有关完整信息，请参阅以下位置的《思科内容安全虚拟设备安装指南》：<http://www.cisco.com/c/en/us/support/security/web-security-appliance/products-installation-guides-list.html>。

## 过程

---

- 步骤 1** 打开浏览器并输入 WSA 的 IP 地址。首次运行“系统设置向导”(System Setup Wizard)时,请使用默认 IP 地址: <https://192.168.42.42:8443> 或 <http://192.168.42.42:8080>, 其中 192.168.42.42 是默认 IP 地址, 8080 是 HTTP 的默认管理端口设置, 8443 是 HTTPS 的默认管理端口。如果已经配置设备, 请使用 M1 端口的 IP 地址。
- 步骤 2** 系统显示设备登录屏幕时, 输入用户名和密码。默认情况下, 设备随附以下用户名和密码:
- 用户名: admin
  - 密码: ironport
- 步骤 3** 选择系统管理 (System Administration) > 系统设置向导 (System Setup Wizard), 打开欢迎页面, 此页面包含四个选项卡: 开始 (Start)、网络 (Network)、安全 (Security) 和检查 (Review)。
- 步骤 4** 如果已经配置设备, 系统将提示您需要重置配置。要继续操作, 请选择系统设置向导 (System Setup Wizard), 点击重置配置 (Reset Configuration) 按钮。设备将重置并且浏览器将刷新为设备主屏幕。
- 步骤 5** 在开始 (Start) 选项卡中, 阅读并接受最终用户许可协议的条款。
- 步骤 6** 点击开始设置 (Begin Setup) 继续操作。
- 步骤 7** 在网络 (Network) 选项卡中, 按照要求使用所提供的参考表配置所有设置。
- 步骤 8** 在安全 (Security) 选项卡中, 配置所有设置。
- 步骤 9** 在检查 (Review) 选项卡中, 检查配置信息。如果您需要更改某个选项, 请点击该部分的编辑 (Edit) 按钮。
- 步骤 10** 点击安装这个配置 (Install This Configuration)。  
安装了配置之后, 系统应该显示后续步骤 (Next Steps) 页面。但是, 根据您在设置期间配置的 IP、主机名或 DNS 设置, 在此阶段您可能会失去与设备的连接。如果浏览器中显示“找不到页面”(“Page not found”)消息, 请更改 URL, 反映所有新地址设置并重新加载页面。然后, 继续执行您想要执行的任何设置后任务。
- 

## 在 WSA 上配置 ISE 功能

### 开始之前

- 获取 ISE 服务器主机名或 IP 地址。
- 如果您使用的是外部生成的证书/密钥组合, 请获取 WSA 客户端身份验证证书和密钥文件。
- 为 WSA 数据初始化获取 ISE 管理员证书。
- 为 WSA 数据订阅获取 ISE pxGrid 证书。

## 过程

- 步骤 1 选择网络 (Network) > 身份服务引擎 (Identity Services Engine)，打开身份服务引擎配置页面。
- 步骤 2 点击编辑设置 (Edit Settings)，添加或更新 WSA 客户端、ISE 管理员和 pxGrid 证书。
- 步骤 3 确认选中启用 ISE 服务 (Enable ISE Service) 复选框，以启用 ISE 服务。
- 步骤 4 使用 ISE 服务器主机名或 IPv4 地址识别 ISE 服务器。
- 步骤 5 选择要用于为 WSA-ISE 服务器相互身份验证提供客户端证书的方法：
  - “使用上传的证书和密钥” (Use Uploaded Certificate and Key) - 如有必要，上传并选择相应文件。
  - 也可以选择“使用生成的证书和密钥” (Use Generated Certificate and Key) - 如有必要，生成新的证书和密钥。
    - 点击生成新的证书和密钥 (Generate New Certificate and Key)。
    - 在生成证书和密钥 (Generate Certificate and Key) 对话框中，输入要在签名证书中显示的信息。
    - 点击生成 (Generate)。
    - 点击下载证书签名请求 (Download Certificate Signing Request) (DCSR) 链接，将其提交至证书颁发机构 (CA)。从 CA 收到签名的证书之后，点击浏览 (Browse) 并导航至签名证书位置。点击上传文件 (Upload File)。
    - 如果 CA root 没有显示，则请在 ISE 服务器上的管理 (Administration) > 证书 (Certificates) > 受信任证书 (Trusted Certificates) 下添加 CA root。
  - 如果用户不希望使用 CA 签名的 WSA 客户端证书：
    - 点击下载证书 (Download Certificate)，然后将证书下载至一个本地文件夹。
    - 在 ISE 服务器中，将此证书上传至管理 (Administration) > 证书 (Certificates) > 受信任证书 (Trusted Certificates)。
- 步骤 6 如果使用的是本地保存的 WSA 客户端证书和密钥，请确保可以在管理 (Administration) > 证书 (Certificates) > 受信任证书 (Trusted Certificates) 路径下找到证书。否则，请在 ISE 服务器管理员用户界面上导航至管理 (Administration) > 证书 (Certificates) > 受信任证书 (Trusted Certificates) > 导入 (Import) 路径，导入证书。
- 步骤 7 提供一个 ISE 管理员证书，用于将 ISE 用户配置文件数据批量下载至 WSA。浏览并选择证书文件，然后点击“上传文件” (Upload Files)。有关更多信息，请参阅[上传根证书和密钥](#)（第 22-25 页）。
- 步骤 8 提供一个 ISE pxGrid 证书，用于订购 WSA-ISE 数据（对 ISE 服务器的持续查询）。浏览并选择证书文件，然后点击“上传文件” (Upload Files)。有关更多信息，请参阅[上传根证书和密钥](#)（第 22-25 页）。
- 步骤 9 （可选）点击开始测试 (Start Test)。此测试将执行以下操作：
  - 将 ISE 主机名解析为其对应的 IP 地址。
  - 验证 WSA 客户端证书。
  - 验证 ISE pxGrid 证书。

- 验证 ISE 管理员证书。
- 检查与 ISE pxGrid 的连接并检索 SGT。
- 检查与 REST 服务器的连接。

**步骤 10** 点击提交 (Submit)，然后点击应用更改 (Commit Changes)。

## WSA 标识配置文件设置

选择 **Web 安全管理器 (Web Security Manager) > 标识配置文件 (Identification Profiles) > 添加标识配置文件 (Add Identification Profile)**，为需要通过 ISE 进行身份验证的 WSA 客户端创建身份配置文件。“标识配置文件” (Identification Profiles) 页面包含以下部分：

部分	说明
客户端/用户标识配置文件	启用标识配置文件： <ul style="list-style-type: none"> <li>• “名称” (Name) - 为标识配置文件输入一个名称。</li> <li>• “说明” (Description) - 输入说明。</li> <li>• “在上方插入” (Insert Above) - 输入匹配策略与传入请求应该遵守的顺序（从上至下）。</li> </ul>
用户识别	“使用 ISE 透明识别用户” (Transparently identify users with ISE) - 用户名和关联的 SGT 将从 ISE 获取。
回退到身份验证领域或访客权限	如果 ISE 无法提供用户身份验证，则可以选择以下选项： <ul style="list-style-type: none"> <li>• “支持访客权限” (Support Guest Privileges) - 用户可以通过 WSA 代理并且以访客身份进行身份验证。</li> <li>• “要求身份验证” (Require Authentication) - 用户可以通过 WSA 代理并且可以使用 Windows NT 局域网管理器 (NTLM)、轻量级目录访问协议 (LDAP)、Kerberos 或透明用户标识 (TUI) 等协议进行身份验证。</li> <li>• “阻止事务” (Block Transactions) - 不允许 ISE 无法识别的用户访问互联网。</li> </ul>

“回退到身份验证领域” (Fallback to Authentication Realm) 或 “访客权限” (Guest Privileges) 选项根据所选选项而更改。

“回退到身份验证领域” (Fallback to Authentication Realm) 或 “访客权限” (Guest Privileges) 选项	说明
支持访客权限	无更改

“回退到身份验证领域” (Fallback to Authentication Realm) 或 “访客权限” (Guest Privileges) 选项	说明
要求身份验证	<p>选择一个领域或序列：</p> <ul style="list-style-type: none"> <li>• authLDAP</li> <li>• ntlmrealm</li> <li>• 所有领域</li> </ul> <p>身份验证代理：</p> <ul style="list-style-type: none"> <li>• “IP 地址” (IP Address) - Web 代理跟踪特定 IP 地址上经过身份验证的用户。对于 TUI，请选择此选项。</li> <li>• “永久性 Cookie” (Persistent Cookie) - Web 代理通过为每个应用的每位用户生成一个永久性 Cookie，跟踪特定应用上经过身份验证的用户。关闭应用并不会清除此 Cookie。</li> <li>• “会话 Cookie” (Session Cookie) - Web 代理通过为每个域内每个应用的每位用户生成一个会话 Cookie，跟踪特定应用上经过身份验证的用户。（但是，当用户从同一应用为相同的域提供不同的凭证时，此 Cookie 会被覆盖。）关闭应用会清除此 Cookie。</li> </ul>
阻止事务	无更改

## 为 WSA 客户端创建身份配置文件

您应为 WSA 客户端创建标识配置文件并向子网 10.4.100.0/24 上的用户分配访客权限。

### 过程

- 步骤 1 选择 **Web 安全管理器 (Web Security Manager) > 标识配置文件 (Identification Profiles) > 添加标识配置文件 (Add Identification Profile)**。
- 步骤 2 在 **启用标识配置文件 (Enable Identification Profile)** 部分，输入必填详细信息。
- 步骤 3 在 **用户标识方法 (User Identification Method)** 部分，选择使用 **ISE 透明识别用户 (Transparently Identify Users with ISE)** 和支持访客权限 (**Support Guest Privileges**)。
- 步骤 4 在 **成员定义 (Membership Definition)** 部分，输入子网地址（例如 10.4.100.0/24）。
- 步骤 5 在 **按协议定义成员 (Define Members by Protocol)** 部分，选择所需选项（例如 **HTTP/HTTPS** 和本机 **FTP (Native FTP)** 选项）。
- 步骤 6
- 步骤 7 点击提交 (**Submit**)。

Client / User Identification Profile Settings	
<input checked="" type="checkbox"/> <b>Enable Identification Profile</b>	
Name: ?	id3IsePolicy <i>(e.g. my IT Profile)</i>
Description:	
Insert Above:	8 (Global Profile) ▾
User Identification Method	
Identification and Authentication: ?	Transparently identify users with ISE ▾
Fallback to Authentication Realm or Guest Privileges: ?	If user information is not available from the Identity Services Engine: Support Guest Privileges ▾ <i>Authorization of specific users and groups is defined in subsequent policy layers (see Web Security Manager &gt; Decryption Policies, Routing Policies and Access Policies).</i>
Membership Definition	
<i>Membership is defined by any combination of the following options. All criteria must be met for the policy to take effect.</i>	
Define Members by Subnet:	10.4.100.0/24 <i>(examples: 10.1.1.0, 10.1.1.0/24, 10.1.1.1-10, 2001:420:80:1::5, 2000:db8::1-2000:db8::10)</i>
Define Members by Protocol:	<input checked="" type="checkbox"/> HTTP/HTTPS <input checked="" type="checkbox"/> Native FTP
▸ <b>Advanced</b>	<i>Define additional group membership criteria.</i>

您还可以选择完全阻止某个用户或终端。

## 为 WSA 客户端创建访问策略

您已为子网 10.4.100.0/24 上的用户创建标识配置文件。您需要确认已从 ISE 检索的 SGT，从而可以将访问策略与所需的 SGT 关联。

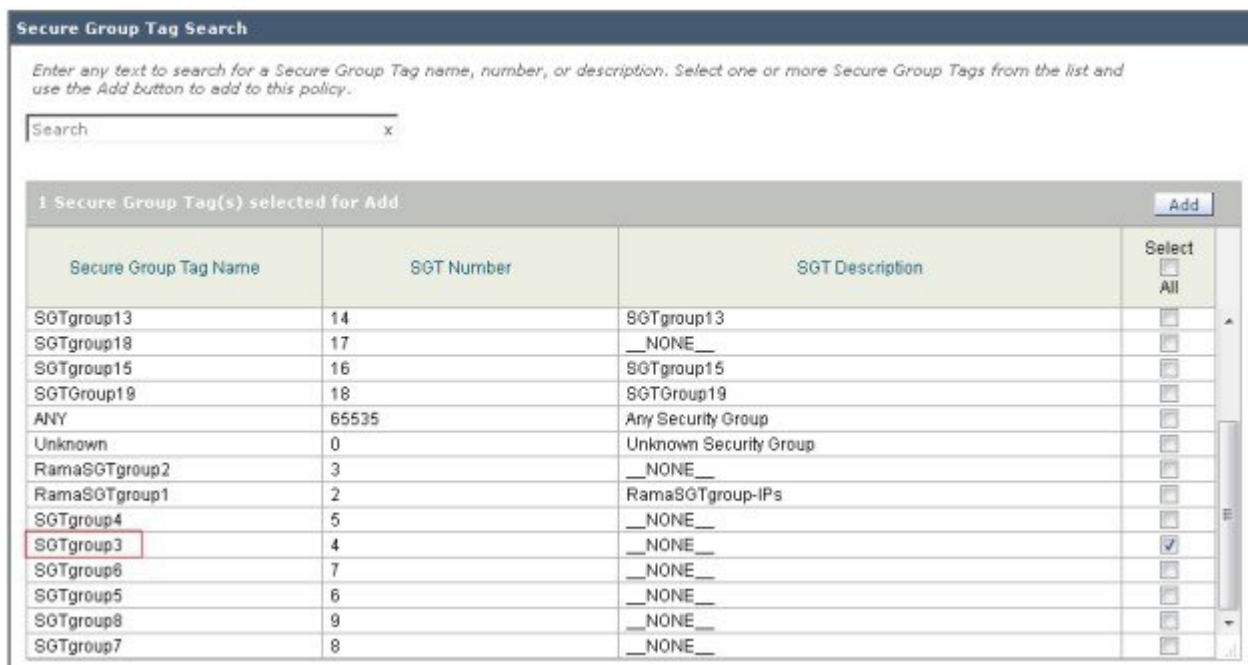


注释 也可以使用 CLI 命令 `isedata` 确认所检索的 ISE SGT。

### 过程

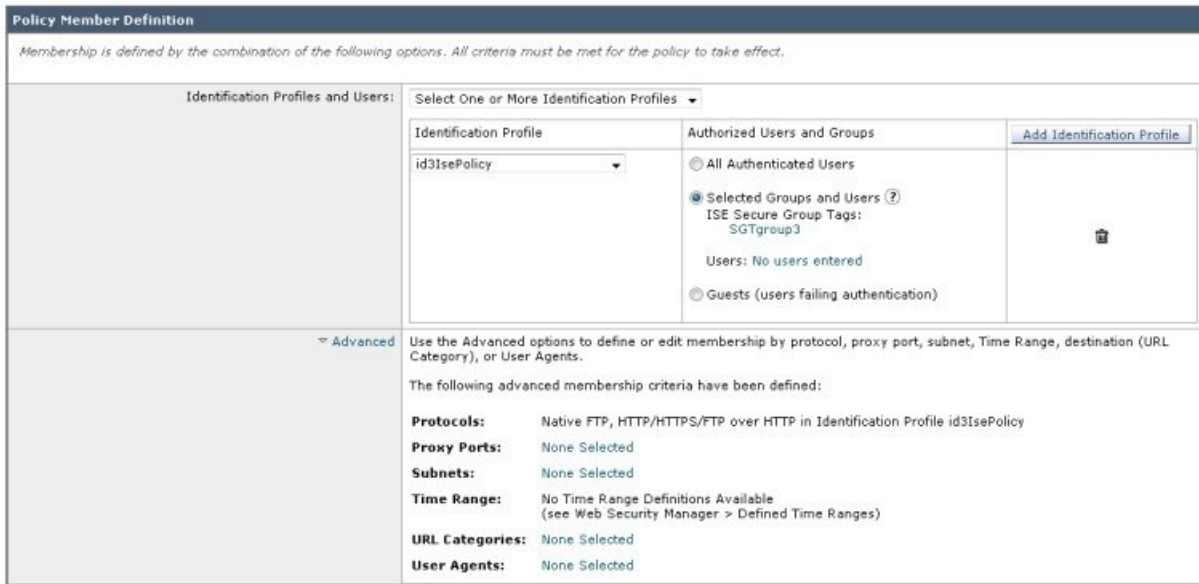
**步骤 1** 选择 **Web 安全管理器 (Web Security Manager) > 访问策略 (Access Policies) > 添加策略 (Add Policy)**。

- 步骤 2** 在策略设置 (Policy Settings) 部分，输入必填详细信息。
- 步骤 3** 在策略成员定义 (Policy Member Definition) 部分，从标识配置文件和用户 (Identification Profiles and Users) 下拉列表选取选择一个或多个标识配置文件 (Select One or More Identification Profiles)。
- 步骤 4** 从选择标识配置文件 (Select Identification Profile) 下拉列表选择您之前创建的策略。
- 步骤 5** 在已授权用户和组 (Authorized Users and Groups) 列中，选择已选组 and 用户 (Selected Groups and Users)。
- 步骤 6** 点击未输入任何标记 (No Tags Entered) 链接，从 ISE 服务器获取 SGT。（此列表与 ISE 策略 (ISE Policy)> 结果 (Results) > Trustsec > 安全组 (Security Groups) 页面相同。）
- 步骤 7** 选择所需的 SGT（例如 SGTgroup3），然后点击添加 (Add)，将所选的 SGT 添加至已授权安全组标记 (Authorized Secure Group Tags) 部分。



- 步骤 8** 点击完成 (Done)，将所选 SGT 添加至访问策略。





WSA 配置文件将链接至您所创建的 SGT。

## 使用 WSA 报告查看用户状态

您为用户创建了身份配置文件和访问策略之后，就可以在用户登录网络时检查其状态。导航至报告 (Reporting) > Web 跟踪 (Web Tracking) 页面，填写必填字段，然后点击搜索 (Search)，即可在结果 (Results) 部分查看输出。例如，如果 User3 已由 ISE 进行身份验证，您可以在报告中查看文本“已由 ISE 识别” (“Identified by ISE”) 以及客户端 IP 地址。对于访客用户和受阻止的 IP 地址，则仅显示客户端 IP 地址。有关完整信息，请参阅《WSA 用户指南》中的“Web 跟踪”页面。

## 使用日志文件对 ISE-WSA 集成问题进行故障排除

WSA 在其日志文件中记录其与系统和流量管理相关的活动。与 ISE-WSA 集成相关的日志为 W3C 日志、访问日志、ISE 日志和代理日志。您可以使用这些日志来监控与集成相关的问题并进行故障排除。

日志文件	功能	WSA GUI 路径	SSH 命令
W3C 日志	以符合 W3C 的格式记录 Web 代理客户端历史记录。	系统管理 (System Administration) > 日志订阅 (Log Subscriptions)	取决于 GUI 配置 - “系统管理” (System Administration) > “日志订阅/日志配置” (Log Subscriptions/logconfig)。
访问日志	记录 Web 代理客户端历史记录。	系统管理 (System Administration) > 日志订阅 (Log Subscriptions) > 访问日志 (accesslogs)	ssh admin@WSA tail ise_service_log

日志文件	功能	WSA GUI 路径	SSH 命令
ISE 日志	记录与使用 ISE 相关的消息，例如与 ISE 服务器通信成功还是失败。	系统管理 (System Administration) > 日志订阅 (Log Subscriptions) > ISE 服务日志 (ise_service_log)	ssh admin@WSA tail ise_service_log
代理日志	记录与 Web 代理相关的错误。这是所有与 Web 代理相关的日志中最基本的功能。要对与 Web 代理相关的更多具体方面进行故障排除，请为适用的 Web 代理模块创建一个日志订用。	系统管理 (System Administration) > 日志订阅 (Log Subscriptions) > 代理日志 (proxylogs)	ssh admin@WSA tail proxylogs

## 访问日志文件 - 示例

以下是可用于故障排除的访问日志文件的一些示例。

### 示例 1: 向无 SGT 的 ISE 缓存中发现的用户应用的访问策略。

```
1424330486.386 320 10.19.75.75 TCP_MISS/200 68632 GET http://www.bing.com/ "user1" DIRECT/www.bing.com text/html
DEFAULT_CASE_12-DefaultGroup-DefaultGroup-NONE-NONE-NONE-DefaultGroup
<IW_srch,6.1,1,"-",-,-,-,1,"-",-,-,-,"-",1,-,"-","-",-,-,IW_srch,-,"-","-","Bing","Search
Engine","-","-",1715.80,0,-,-,"-","-",1,"-",-,-,"-","-> - SSO_ISE
```

### 示例 2: 向有匹配 SGT 的 ISE 缓存中的用户应用的访问策略。

```
1424331112.566 0 10.19.75.75 TCP_DENIED/403 0 GET http://www.bing.com/ "user1" NONE/- -
BLOCK_WEBCAT_12-BYODPolicy-DefaultGroup-NONE-NONE-NONE-NONE
<IW_srch,6.1,-,"-",-,-,-,"-",-,-,-,"-","-",-,-,IW_srch,-,"-","-","Unknown","Unknown","-","-",0.00,0,-,-,"-","-","-","-","-","->
- SSO_ISE
```

### 示例 3: 具有回退到访客的功能的访问策略

```
1424330523.414 155 172.29.177.25 TCP_MISS/200 68647 GET http://www.bing.com/ "(Unauthenticated)172.29.177.25"
DIRECT/www.bing.com text/html DEFAULT_CASE_12-DefaultGroup-Default
Group-NONE-NONE-NONE-DefaultGroup
<IW_srch,6.1,1,"-",-,-,-,1,"-",-,-,-,"-",1,-,"-","-",-,-,IW_srch,-,"-","-","Bing","Search
Engine","-","-",3543.07,0,-,-,"-","-",1,"-",-,-,"-","-
"> - GUEST
```

### 示例 4: 具有回退到阻止事务的功能的访问策略

```
1424331683.561 0 172.29.177.25 TCP_DENIED/403 0 GET http://www.bing.com/ - NONE/- -
OTHER-NONE-DefaultGroup-NONE-NONE-NONE-NONE
<,-,-,-,"-",-,-,-,-,"-","-","-","-","-","-",0.00,0,-,-,"-","-","-","-","-","->
- NONE
```

## ISE 日志文件 - 示例

以下是可用于故障排除的 ISE 日志文件的一个示例。

```
Thu Mar 12 20:41:29 2015 Info: Begin Logfile
Thu Mar 12 20:41:30 2015 Info: ISEService: Successfully loaded configuration from: /data/ise/ise_service.ini
```

```

Thu Mar 12 20:41:30 2015 Info: ISEService: RPC Server Socket :/tmp/ise_fastrpc.sock
Thu Mar 12 20:41:30 2015 Info: RPCServer: Starting at: /tmp/ise_fastrpc.sock
Thu Mar 12 20:41:30 2015 Info: ISEService: Running
Thu Mar 12 20:41:30 2015 Info: ISEDynamicConfigThread: Started Server..
Thu Mar 12 20:41:30 2015 Info: ISEService: Sending ready signal...
Thu Mar 12 20:41:31 2015 Info: ISEBulkDownloader: Downloaded 12 SGTs in 0.162157773972 seconds
Thu Mar 12 20:41:32 2015 Info: ISEBulkDownloader: Downloaded 0 sessions in 0.316617965698 seconds

```

## 对 ISE-WSA 集成问题进行故障排除 - ISE 服务器连接

本节介绍在将 ISE 与 WSA 集成期间您可能会遇到的问题。

- 网络问题：您可能会遇到与所配置的 ISE 服务器端口的连接问题。例如，您可能会遇到端口 5222 的防火墙问题。您可以使用 telnet 和 tcpdump 命令，调试网络问题。

- 证书问题：

证书	在以下情况下，您可能会遇到问题：
由 CA 签名	<ul style="list-style-type: none"> <li>• WSA 中没有管理员或 pxGrid 证书根 CA。</li> <li>• ISE 受信任证书库 (ISE Trusted Certificates Store) 中没有给 WSA 客户端证书签名的根 CA。</li> </ul>
自签名	<ul style="list-style-type: none"> <li>• ISE 受信任证书库 (ISE Trusted Certificates Store) 中没有 WSA 客户端证书。</li> <li>• WSA 中没有 ISE 管理员或 pxGrid 证书。</li> </ul>
全部	<ul style="list-style-type: none"> <li>• 上传期间有效的证书在当前日期已经过期。</li> </ul>

- 身份映射查询问题：您可能会在以下方面遇到问题：

- 从 ISE 服务器下载 SGT 时遇到问题，尽管在端口 443 上 SSL 握手成功。您应该在 ISE 服务器上调试该问题。
- WSA 拒绝经过 ISE 身份验证的用户访问。使用 sedata cache 和 isedata statistics 命令。

- 数据包捕获：您可以捕获和显示 TCP/IP 数据包以及在设备所连接的网络上传输或接收的其他数据包。请参阅《[WSA 用户指南](#)》中的“数据包捕获” (Packet Capture) 页面。

- 策略跟踪：请参阅《[WSA 用户指南](#)》中的“跟踪客户端请求” (Tracing Client Requests) 页面。

## 与 ISE-WSA 集成有关的 SMA 的概述

思科内容安全管理设备 (SMA) 是一个统一的管理平台，可以管理 Web 安全，执行故障排除，以及为数月乃至数年的数据存储维护空间。它是一种集中式系统，用于统一管理和报告网络中部署的 WSA。例如，如果部署中有五个 WSA，在 SMA 上显示的报告将是这所有 WSA 的一个合并报告。将报告分配至 SMA 之后，您将无法在 WSA 上查看报告。只有在关联 WSA 上支持某项功能时，在 SMA 上才会支持此功能。

SMA 包含的信息与 WSA 是否配置了 ISE 相关。如果配置了 ISE，则 SMA 包含与 SGT 相关的信息。您可以利用 SGT 在 SMA 上创建 WSA 策略。SMA 定期更新与 ISE 相关的信息，大约每 5 分钟更新一次。您可以创建一个标准配置，并在部署中的所有 WSA 上发布。SMA 图形用户界面 (GUI) 与 WSA 类似，但是具有一些独特的功能。

在 SMA 中，选择 **Web > 实用程序 (Utilities) > Web 设备状态 (Web Appliance Status)**，然后点击相应的 WSA，即可发现是否已启用 ISE。





美洲总部  
Cisco Systems, Inc.  
San Jose, CA 95134-1706  
USA

亚太区总部  
Cisco Systems (USA) Pte. Ltd.  
Singapore

欧洲总部  
Cisco Systems International BV  
Amsterdam, The Netherlands

Cisco 在全球拥有 200 多个办事处。相关地址、电话和传真号码可见于  
Cisco 位于 [www.cisco.com/go/offices](http://www.cisco.com/go/offices) 上的网站。