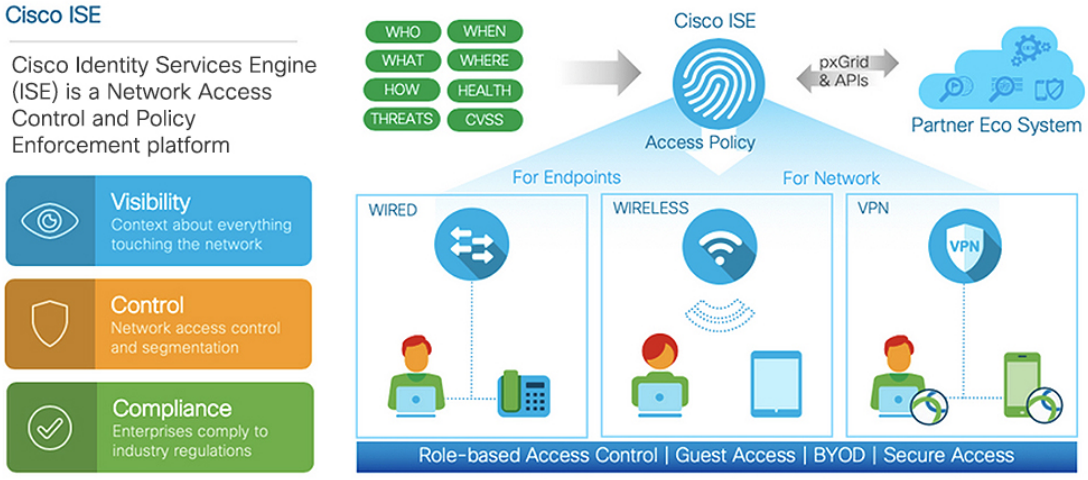
概述

思科 ISE 概述



Cisco身份服务引擎 (ISE) 是一个基于身份的网络访问控制和策略实施系统。它作为一个通用策略引擎，让企业能够控制终端访问和管理网络设备。

您可以利用Cisco ISE 确保合规、增强基础设施安全性并简化服务操作。

Cisco ISE管理员可以收集网络的实时情景数据，包括用户和用户组（谁？）、设备类型（什么？）、访问时间（何时？）、访问位置（哪里？）、访问类型（有线、无线或 VPN）（如何？）以及网络威胁和漏洞。

作为Cisco ISE 管理员，您可以使用此信息制定网络监管决策。您还可以将身份数据与各种网络元素绑定，以创建监管网络访问和使用的策略。

思科 ISE 功能

Cisco ISE 软件必须按原样安装。不能在底层操作系统级别安装任何其他第三方应用。

Cisco ISE 为您提供以下功能：

- **设备管理 (Device Administration)**：Cisco ISE 使用 TACACS+ 安全协议来控制和审核网络设备的配置。它可以促进对谁可以访问哪个网络及更改关联网络设置进行精细控制。网络设备可以配置为向Cisco ISE 查询对设备管理员操作所进行的身份验证和授权。这些设备还会向Cisco ISE 发送记账消息，以记录此类操作。
- **访客和安全无线 (Guest and Secure Wireless)**：Cisco ISE 使您能够为访客、承包商、顾问和客户提供安全的网络访问。您可以使用基于 Web 的门户和移动门户将访客加入公司的网络和内部资源。您可以为不同类型的访客定义访问权限，并分配发起人以创建和管理访客帐户。
- **自带设备 (BYOD) (Bring Your Own Device [BYOD])**：Cisco ISE 可以让您的员工和访客在企业网络上安全地使用他们的个人设备。BYOD功能的最终用户可以使用所配置的路径添加其设备，并调配预定义的身份验证和网络访问级别。
- **资产可视性 (Asset Visibility)**：Cisco ISE 在无线连接、有线连接和 VPN 连接中提供一致的可视性，并控制网络上的人员和内容。Cisco ISE 使用探测器和设备传感器来侦听设备连接到网络的方式。然后，庞大的Cisco ISE 配置文件数据库将对设备进行分类。这可以提供您所需要的可视性和情景，以便授予适当级别的网络访问权限。
- **安全有线访问 (Secure Wired Access)**：Cisco ISE 使用各种身份验证协议为网络设备和终端提供安全的有线网络访问。这些协议包括但不限于802.1X、RADIUS、MAB、基于Web、EasyConnect 和启用外部代理的身份验证方法。
- **分段 (Segmentation)**：Cisco ISE 使用有关网络设备和终端的情景数据来促进网络分段。安全组标记、访问控制列表、网络访问协议，以及用来定义授权、访问和身份验证的策略集是Cisco ISE 实现安全网络分段的一些方式。
- **终端安全评估或合规性 (Posture or Compliance)**：Cisco ISE 可以让您检查终端的合规性（也称为终端安全评估），然后再允许它们连接您的网络。您可以确保终端接收适当的终端安全评估代理以提供终端安全评估服务。
- **威胁遏制 (Threat Containment)**：如果Cisco ISE 检测到来自终端的威胁或漏洞属性，则发送自适应网络控制策略以动态更改其终端访问级别。在评估并解决威胁或漏洞后，终端将获得其原始访问策略。
- **安全生态系统集成 (Security Ecosystem Integrations)**：通过 pxGrid 功能，Cisco ISE 可以与相连的网络设备、第三方供应商或Cisco合作伙伴系统安全地共享情景相关信息、策略和配置数据等。

思科 ISE 管理员

管理员可使用管理员门户执行下列操作：

- 管理部署、服务中心操作、网络设备以及节点监控和故障排除。
- 管理Cisco ISE 服务、策略、管理员帐户以及系统配置和操作。
- 更改管理员和用户密码。

CLI 管理员可以启动和停止Cisco ISE 应用、应用软件补丁和升级、重新加载或关闭Cisco ISE 设备，以及查看所有系统和应用日志。由于授予 CLI 管理员的特殊权限，建议您保护 CLI 管理员凭证并创建基于 Web 的管理员来配置和管理Cisco ISE 部署。

在设置过程中配置的用户名和密码仅用于对 CLI 进行管理访问。此角色被视为 CLI 管理员用户，也称为CLI管理员。默认情况下，CLI管理员用户的用户名为admin，密码是设置过程中定义的密码。没有默认密码。此 CLI 管理员用户是默认管理员用户，无法删除此用户帐户。不过，其他管理员可以编辑此用户帐户，包括启用、禁用或更改此帐户密码的选项。

可以创建管理员，也可以将现有用户升级为管理员角色。通过禁用对应的管理权限，还可以将管理员降级为简单网络用户状态。

管理员是具有配置和操作Cisco ISE 系统的本地权限的用户。

管理员会分配到一个或多个管理员组。

相关主题

思科 ISE 管理员组，第 5 页

强制 CLI 管理员使用外部身份存储库

使用外部身份源进行身份验证比使用内部数据库更安全。适用于 CLI 管理员的 RBAC 支持外部身份库。

必备条件

您必须已定义管理员用户，并将其添加到管理员组。管理员必须是超级管理员。

在 AD 用户目录中定义用户的属性

在运行 Active Directory 的 Windows 服务器上，修改您计划配置为 CLI 管理员的每个用户的属性。

1. 打开服务器管理器窗口，然后导航至**服务器管理器 (Server Manager) > 角色 (Roles) > Active Directory 域服务 (Active Directory Domain Services) > Active Directory 用户和计算机 (Active Directory Users and Computers) > [ad.adserver]<ad_server> .local**。
2. 在**视图 (View)** 菜单下启用**高级功能 (Advanced Features)**，以便您编辑用户的属性。
3. 导航至包含管理员用户的 Active Directory 组，并找到该用户。

4. 双击用户以打开**属性 (Properties)** 窗口并选择**属性编辑器 (Attribute Editor)**。
5. 点击任意属性并开始键入“gid”以查找属性 `gidNumber`。如果找不到gidNumber属性，请点击**过滤器 (Filter)** 按钮并取消选中**仅显示具有值的属性 (Show only attributes that have values)**。
6. 双击属性名称以编辑每个属性。对于每个用户：
   - 分配大于 60000 的 `uidNumber`，并确保该数字是唯一的。
   - 将 `gidNumber` 分配为 110 或 111。
   - GidNumber 110 表示管理员用户，而 111 表示只读用户。
   - 请勿在分配后更改 uidNumber。
   - 如果修改 gidNumber，请至少等待五分钟，然后再建立 SSH 连接。

将管理员 CLI 用户加入 AD 域

连接到Cisco ISE CLI，运行 **identity-store** 命令，并将管理员用户分配到 ID 存储区。例如，要将 CLI 管理员用户作为 adpool1 映射到 ISE 中定义的 Active Directory，请运行 **identity-store active-directory domain-name adpool1 user admincliuser**。

完成加入后，连接到Cisco ISE CLI 并以管理员 CLI 用户身份登录，验证您的配置。

如果在此命令中使用的域之前已加入 ISE 节点，则必须在管理员控制台中重新加入该域。

1. **管理 (Administration) > 身份管理 (Identity Management) > 外部身份源 (External Identity Sources)**。
2. 在左侧窗格中，选择 **Active Directory** 并选择您的 Active Directory 名称。
3. 在右侧窗格中，您的 AD 连接的状态可能显示**运行 (Operational)**。但是，如果使用 MS-RPC 或 Kerberos，通过**测试用户 (Test User)** 测试连接，则会收到错误。
4. 验证您是否仍可以用管理员 CLI 用户身份登录Cisco ISE CLI。

创建新管理员

Cisco ISE 管理员需要分配有特定角色的帐户才能执行特定管理任务。可以创建管理员帐户，并根据管理员必须执行的管理任务向这些管理员分配一个或多个角色。

可以使用**管理员用户 (Admin Users)** 窗口查看、创建、修改、删除、复制或搜索Cisco ISE 管理员的属性或更改其状态。

注释 如果管理员用户的域在 CLI 和 GUI 中相同，建议您先在 CLI 中配置 Active Directory 访问权限，然后再将其加入 GUI。另外，必须从 GUI 重新加入域，以避免此域发生身份验证失败。

步骤 1 选择 管理 **(Administration)** > 系统 **(System)** > 管理员访问权限 **(Admin Access)** > 管理员 **(Administrators)** > 管理员用户 **(Admin Users)** > 添加 **(Add)**。

步骤 2 管理 **(Administration)** > 系统 **(System)** > 管理员访问权限 **(Admin Access)** > 管理员 **(Administrators)** > 管理员用户 **(Admin Users)** > 添加 **(Add)**

步骤 3 从下拉列表中，选择以下选项之一：

- **创建管理员用户 (Create an Admin User)**

  如果选择**创建管理员用户 (Create an Admin User)**，将显示**新建管理员 (New Administrator)** 窗口，从中可配置新管理员用户的帐户信息。

- **从网络访问用户选择 (Select from Network Access Users)**

  如果选择**从网络访问权限用户中选择 (Select from Network Access Users)**，将显示当前用户列表，从中可创建用户。将显示与此用户对应的**管理员用户 (Admin User)** 窗口。

步骤 4 在字段中输入值。**名称 (Name)** 字段支持的字符为 # $ ’ ( ) * + -。/ @ _。

管理员用户名必须唯一。如果输入了现有用户名，错误弹出窗口将显示以下消息：

无法创建用户。已存在具有相同名称的用户。(User can't be created. A User with that name already exists.)

步骤 5 点击**提交 (Submit)** 在Cisco ISE 内部数据库中创建新管理员。

相关主题

只读管理员策略，第 20 页
创建内部只读管理员
自定义只读管理员的菜单访问权限，第 20 页
将外部组映射至只读管理员组

思科 ISE 管理员组

管理员组是CiscoISE中基于角色的访问控制（RBAC）组。属于同一组的所有管理员共用同一身份并且具有相同的权限。管理员作为特定管理组成员的身份可用作授权策略中的条件。管理员可以属于不止一个管理员组。

具有任何访问权限级别的管理员帐户可以在其有权访问的任何窗口上，修改或删除其拥有权限的对象。

在Cisco ISE 安全模式下，管理员只能创建与其具有相同权限集的管理组。提供的权限基于Cisco ISE 数据库中定义的用户管理角色。这样，管理组就形成了定义访问Cisco ISE 系统的权限的依据。

下表列出了Cisco ISE 中预定义的管理组以及这些组成员可以执行的任务。

表 *1:* 思科 *ISE* 管理员组、访问级别、权限和限制

管理组角色	访问级别	权限	限制
自定义管理员	管理发起人、访客和个人设备门户。	• 配置访客和发起人访问权限。 • 管理访客访问设置。 • 自定义最终用户 Web 门户。	• 无法在Cisco ISE 中执行任何策略管理、身份管理或系统级别配置任务。 • 无法查看任何报告
帮助台管理员	查询监控和故障排除操作	• 运行所有报告。 • 运行所有故障排除流程。 • 查看Cisco ISE 控制板和实时日志。 • 查看警报。	无法创建、更新或删除报告、故障排除流程、实时身份验证或警报。
身份管理员	• 管理用户帐户和终端。 • 管理身份源。	• 添加、编辑和删除用户帐户和终端。 • 添加、编辑和删除身份源。 • 添加、编辑和删除身份源序列。 • 为用户帐户配置常规设置（属性和密码策略）。 • 查看Cisco ISE 控制板、实时日志、警报和报告。 • 运行所有故障排除流程。	无法在Cisco ISE 中执行任何策略管理或系统级别配置任务。

管理组角色	访问级别	权限	限制
MnT 管理员	执行所有监控和故障排除操作。	• 管理所有报告（运行、创建和删除）。 • 运行所有故障排除流程。 • 查看Cisco ISE 控制板和实时日志。 • 管理警报（创建、更新、查看和删除）。	无法在Cisco ISE 中执行任何策略管理、身份管理或系统级别配置任务。
网络设备管理员	管理Cisco ISE 网络设备和网络设备存储库。	• 对网络设备拥有读写权限 • 对网络设备组和所有网络资源对象类型拥有读写权限。 • 查看Cisco ISE 控制板、实时日志、警报和报告。 • 运行所有故障排除流程。	无法在Cisco ISE 中执行任何策略管理、身份管理或系统级别配置任务。

管理组角色	访问级别	权限	限制
策略管理员	为所有与身份验证、授权、终端安全评估、分析器和客户端调配和工作中心有关的跨网络 Cisco ISE 服务创建和管理策略。	• 对策略中使用的所有元素（例如授权配置文件、NDG 和条件）拥有读写权限。 • 对身份、终端和身份组（用户身份组和终端身份组）拥有读写权限。 • 对服务策略和设置拥有读写权限。 • 查看Cisco ISE 控制板、实时日志、警报和报告。 • 运行所有故障排除流程。 • 设备管理 - 对设备管理工作中心拥有访问权限。对 TACACS 策略条件和结果拥有权限。TACACS 代理和代理序列的网络设备权限。	无法在Cisco ISE 中执行任何身份管理或系统级别配置任务 设备管理 - 能够访问工作中心并不保证能够访问从链路。

管理组角色	访问级别	权限	限制
RBAC 管理员	**操作 (Operations)** 菜单下除终端保护服务 (Endpoint Protection Services) 自适应网络控制 (Adaptive Network Control) 之外的所有任务，以及对**管理 (Administration)** 下某些菜单项的部分访问权限。	• 查看身份验证详细信息。 • 启用或禁用终端保护服务 (Endpoint Protection Services) 自适应网络控制 (Adaptive Network Control) • 创建、编辑和删除警报；生成和查看报告；以及使用 Cisco ISE 对网络中的问题进行故障排除。 • 对管理员帐户设置和管理组设置拥有读取权限 • 对管理员访问和数据访问权限以及 RBAC 策略页面拥有查看权限。 • 查看Cisco ISE 控制板、实时日志、警报和报告。 • 运行所有故障排除流程。	无法在Cisco ISE 中执行任何身份管理或系统级别配置任务

管理组角色	访问级别	权限	限制
只读管理员	对 ISE GUI 拥有只读访问权限。	• 查看并使用控制板、报告以及实时日志或会话的功能，例如过滤数据、查询、保存选项、打印和输出数据。 • 更改其自有帐户的密码。 • 使用全局搜索、报告以及实时日志或会话查询 ISE。 • 基于属性过滤并保存数据。 • 导出与身份验证策略、配置文件策略、用户、终端、网络设备、网络设备组、身份（包括组）及其他配置相关的数据。 • 自定义报告查询，保存、打印和导出这些查询。 • 生成自定义报告查询，保存、打印或导出结果。 • 保存UI设置以供将来参考。 • 从以下位置下载 ise-psc-log 等日志：**操作 (Operations)** > **故障排除 (Troubleshoot)** > **下载日志 (Download Logs)** 窗口。	

管理组角色	访问级别	权限	限制
			• 对各种对象（例如授权策略、身份验证策略、终端安全评估策略、分析器策略、终端和用户）执行任何配置更改，例如创建、更新、删除、导入、隔离以及移动设备管理 (MDM) 操作。 • 执行系统操作，例如备份和恢复；节点注册或注销；节点同步；创建、编辑和删除节点组；或升级和安装补丁。 • 导入与策略、网络设备、网络设备组、身份（包括组）及其他配置相关的数据。 • 执行操作，例如 CoA、终端调试、修改收集过滤器、绕过实时会话数据的抑制、修改 PAN-HA 故障转移设置，以及编辑 Cisco ISE 节点的角色或服务。 • 运行可能会对性能造成严重影响的命令。例如，访问**操作 (Operations)** > **故障排除 (Troubleshoot)** > **诊断 (Diagnostic)** > **常规工具 (General Tools)** 窗口中的 TCP

管理组角色	访问级别	权限	限制
			转出会受限制。 • 生成支持捆绑包。
超级管理员	所有Cisco ISE 管理功能。默认管理员帐户属于此组。	对所有Cisco ISE 资源拥有创建、读取、更新、删除和执行 (CRUDX) 权限。 **注释** 超级管理员用户无法修改系统生成的默认 RBAC 策略和权限。要执行此操作，您必须根据您的需要利用必要的权限创建新的 RBAC 策略，并且将这些策略映射至管理员组。 设备管理 - 对设备管理工作中心的访问权限。对 TACACS 策略条件和结果拥有权限。TACACS 代理和代理序列的网络设备权限。此外，启用 TACACS 全局协议设置的权限。	• 设备管理 - 能够访问工作中心并不保证能够访问从属链接。 • 只有默认超级管理员组的管理员用户才能修改或删除其他管理员用户。即使是管理员组中克隆有超级管理员组的菜单和数据访问权限的外部映射用户也无法修改或删除管理员用户。

管理组角色	访问级别	权限	限制
系统管理员	所有Cisco ISE 配置和维护任务。	拥有执行**操作 (Operations)** 选项卡下所有活动的完全访问权限（读写权限），以及对**管理 (Administration)** 选项卡下某些菜单项的部分访问权限： • 对管理员帐户设置和管理员组设置拥有读取权限。 • 对管理员访问和数据访问权限以及 **RBAC 策略 (RBAC policy)** 窗口拥有读取权限。 • 对以下位置下方的所有选项拥有读取和访问权限： **管理 (Administration)** > **系统 (System)**。 • 查看身份验证详细信息。 • 启用或禁用终端保护服务 (Endpoint Protection Services) 自适应网络控制 (Adaptive Network Control) • 创建、编辑和删除警报；生成和查看报告；以及使用 Cisco ISE 对网络中的问题进行故障排除。 • 设备管理 - 启用 TACACS 全局协议设置的权限。	无法在Cisco ISE 中执行任何策略管理或系统级别配置任务。

管理组角色	访问级别	权限	限制
升级的系统管理员（在 Cisco ISE 版本 2.6 补丁 2 及更高版本中提供）	所有Cisco ISE 配置和维护任务。	除了系统管理员的所有权限外，升级的系统管理员还可以创建管理员用户。	• 无法创建或删除超级管理员用户。 • 无法管理超级管理员组。
外部 RESTful 服务 (ERS) 管理员	对所有 ERS API 请求（GET、POST、DELETE、PUT）的完全访问权限	• 创建、读取、更新和删除 ERS API 请求。	此角色仅适用于支持 ERS 授权的内部用户、身份组、终端、终端组和 SGT
外部 RESTful 服务 (ERS) 运算符	对 ERS API、仅 GET 的只读访问权限	• 只能读取 ERS API 请求	此角色仅适用于支持 ERS 授权的内部用户、身份组、终端、终端组和 SGT。
TACACS+ Admin	完全访问权限	访问： • 设备管理工作中心。 • 部署 - 启用 TACACS+ services。 • 外部身份存储库。 • **操作 (Operations)** > **TACACS 实时日志 (TACACS Live Logs)** 窗口。	—

相关主题

思科 ISE 管理员，第 3 页

创建管理员组

管理员组 (Admin Groups) 窗口允许您查看、创建、修改、删除、复制或过滤Cisco ISE 网络管理员组。

开始之前

要配置外部管理员组类型，您必须已经指定了一个或多个外部身份库。

步骤 1 选择 **管理 (Administration)** > **系统 (System)** > **管理员访问 (Admin Access)** > **管理员 (Administrators)** > **管理员组 (Admin Groups)**。

步骤 2 点击**添加 (Add)**，并输入名称和说明。

名称 (Name) 字段支持的特殊字符包括：空格、# $ & ‘ ( ) * + -。/ @ _。

步骤 3 指定您所配置的管理员组类型：

- 内部 (Internal)：分配到此组类型的管理员将对存储在Cisco ISE 内部数据库中的凭证进行身份验证。
- 外部 (External)：分配给此组的管理员根据您在**管理 (Administration) > 系统 (System) > 管理员访问 (Admin Access) > 身份验证 (Authentication) > 身份验证方式 (Authentication Method)** 窗口中选择的外部身份库中存储的凭证进行身份验证。如果需要，您可以指定外部组。

如果内部用户配置了用于身份验证的外部身份库，则在登录到 ISE 管理员门户时，内部用户必须选择外部身份库作为**身份源**。如果选择了**内部身份源 (Internal Identity Source)**，身份验证将失败。

步骤 4 点击**成员用户 (Member Users)** 区域中的**添加 (Add)** 将用户添加到此管理员组。

步骤 5 点击 **提交 (Submit)**。

要删除管理员组中的用户，请选中您希望删除的用户所对应的复选框，并点击**删除 (Remove)**。

对思科 ISE 的管理访问

Cisco ISE 管理员可以根据其所属的管理组执行各种管理任务。这些管理任务至关重要。仅向有权在网络中管理 Cisco ISE 的用户授予管理访问权限。

利用Cisco ISE，您可以通过以下选项控制对其 Web 界面的管理访问。

注释 当将Cisco ISE服务器添加到网络时，一旦其Web界面出现，它就会被标记为处于运行状态。但是，由于一些高级服务（如终端安全评估服务）可能需要更长的时间才能完全可用，因此可能需要更多时间才能使所有服务完全运行。

管理访问方法

有多种方式可以连接到 Cisco ISE 服务器。PAN 运行管理员门户，需要管理员密码才能登录。其他 ISE 角色服务器可通过 SSH 或控制台（在其中运行 CLI）进行访问。本节介绍可用于每种连接类型的进程和密码选项。

- **管理员密码**：默认情况下，安装期间创建的 Cisco ISE 管理员用户在 45 天内超时。为防止此情况，可以在以下位置通过关闭密码有效期： **管理 (Administration)** > **系统 (System)** > **管理设置 (Admin Settings)**。点击**密码策略 (Password Policy)** 选项卡，并取消选中**密码有效期 (Password Lifetime)** 下的**管理密码到期 (Administrative passwords expire)**。

如果不执行此操作，当密码到期时，可以在 CLI 中运行 **application reset-passwd** 命令以重置管理员密码。要重置管理密码，可以连接至控制台以访问 CLI，或重新引导 ISE 映像文件以访问引导选项菜单。

- **CLI 密码 (CLI password)**：必须在安装期间输入 CLI 密码。如果在登录 CLI 时因密码无效而遇到问题，可以重置 CLI 密码。连接至控制台，并运行 **password** CLI 命令以重置密码。有关详细信息，请参阅《*ISE CLI* 参考》。
- **SSH 访问 CLI (SSH access to the CLI)**：可以在安装期间或安装后使用 **service sshd** 命令启用 SSH 访问。还可以强制 SSH 连接使用密钥。请注意，在执行此操作时，SSH 与所有网络设备的连接也会使用此密钥，请参阅SSH 密钥验证。可以强制 SSH 密钥使用 Diffie-Hellman 算法。请注意，SSH 密钥不支持 ECDSA 密钥。

思科 ISE 中基于角色的管理员访问控制

Cisco ISE 提供角色型访问控制 (RBAC) 策略，通过限制管理权限确保安全性。RBAC 策略与默认管理组关联，以定义角色和权限。每个预定义管理组都配有一套标准权限（适用于菜单和数据访问），因此，与关联的角色和工作职能保持一致。

用户界面中的某些功能要求具备特定权限才可使用。如果功能不可用，或者不允许您执行特定任务，您的管理组可能没有执行利用此功能的任务所需的权限。

无论访问权限级别如何，任何管理员帐户都可以在任何它能够访问的页面上，修改或删除其拥有权限的对象。

注释 只有具有超级管理员或只读管理员权限的系统定义管理员用户才能查看不属于用户组的基于身份的用户。如果创建的管理员没有这些权限，将无法看到这些用户。

基于角色的权限

Cisco ISE 允许您在菜单和数据级别配置权限：它们称为菜单访问权限和数据访问权限。

菜单访问权限允许您显示或隐藏Cisco ISE 管理界面的菜单项和子菜单项。您可以通过此功能创建权限，从而限制或允许菜单级别的访问。

通过数据访问权限，您可以允许读/写访问、只读访问或禁止访问Cisco ISE 界面中以下数据：管理员组 (Admin Groups)、用户身份组 (User Identity Groups)、终端身份组 (Endpoint Identity Groups)、位置 (Locations) 和设备类型 (Device Types)。

RBAC 策略

RBAC 策略确定是否可以授予管理员对菜单项或其他身份组数据元素的特定类型的访问权限。可以使用 RBAC 策略基于管理员组向管理员授予或拒绝对菜单项或身份组数据元素的访问权限。当管理员登录到管理门户时，他们可以访问基于为与其关联的管理员组定义的策略和权限的菜单和数据。

RBAC 策略将管理员组映射到菜单访问权限和数据访问权限。例如，您可以防止网络管理员查看 Admin Access 操作菜单和策略数据元素。通过为与网络管理员关联的管理员组创建自定义 RBAC 策略，可以实现此目的。

注释 如果使用自定义 RBAC 策略授予或拒绝管理员访问权限，请确保对给定的数据访问权限提供所有相关的菜单访问权限。例如，要添加或删除具有身份或策略管理员数据访问权限的终端，必须提供对**工作中心 (Work Center) > 网络访问 (Network Access)** 以及**管理 (Administration) > 身份管理 (Identity Management)** 的菜单访问权限。

默认菜单访问权限

Cisco ISE 提供一组与一系列预定义的管理员组相关联的现成权限。通过预定义管理员组权限，您可以设置权限，以便任意管理员组的成员可以完全或有限地访问管理界面中的菜单项（称为菜单访问权限）和委派管理员组使用其他管理员组的数据访问要素（称为数据访问权限）。这些权限可进一步用于制定多种管理员组的 RBAC 策略的可重用的实体。Cisco ISE 提供已用于默认 RBAC 策略的一组系统定义的菜单访问权限。除了预定义的菜单访问权限外，Cisco ISE 还允许您在 RBAC 策略中使用的自定义菜单访问权限。钥匙图标表示菜单和子菜单的菜单访问权限，带叉号的钥匙图标表示不同 RBAC 组不可访问的菜单项。

注释 对于超级管理员用户，所有菜单项均可用。对于其他管理员用户，**菜单访问权限 (Menu Access Privileges)** 列中的所有菜单项均可供独立部署及分布式部署中的主要节点使用。对于分布式部署中的辅助节点，**“管理”(Administration)** 选项卡下的菜单项不可用。

配置菜单访问权限

Cisco ISE 允许创建可映射到 RBAC 策略的自定义菜单访问权限。根据管理员的角色，您可以仅允许其访问特定菜单选项。

步骤 1 选择 **管理 (Administration) > 系统 (System) > 管理员访问 (Admin Access) > 授权 (Authorization) > 权限 (Permissions) > 菜单访问 (Menu Access)**。

步骤 2 点击**添加 (Add)**，输入**名称 (Name)** 和**说明 (Description)** 字段的值。

a) 将 **ISE 导航结构 (ISE Navigation Structure)** 菜单展开至所需级别，然后点击要为其创建权限的选项。

b) 在**菜单访问的权限 (Permissions for Menu Access)** 窗格中，点击**显示 (Show)**。

步骤 3 点击**提交 (Submit)**。

授予数据访问权限的先决条件

当 RBAC 管理员对某个对象（例如，用户身份组数据类型的 Employee）具有完全访问权限时，管理员可以查看、添加、更新和删除属于该组的用户。确保管理员已为**用户 (Users)** 窗口（**管理**

[Administration] > 身份管理 [Identity Management] > 身份 [Identities] > 用户 [Users]）授予菜单访问权限。这适用于网络设备和终端对象（基于授予网络设备组和终端身份组数据类型的权限）。

不能对属于默认网络设备组对象（**所有设备类型 [All Device Types]** 和**所有位置 [All Locations]**）的网络设备启用或限制数据访问。如果向在这些默认网络设备组对象下创建的对象授予完全访问数据权限，则显示所有网络设备。因此，我们建议您为网络设备组数据类型创建一个独立于默认网络设备组对象的单独层次结构。您应将网络设备对象分配给新创建的网络设备组，以创建受限访问。

注释　只能为用户身份组、网络设备组和终端身份组启用或限制数据访问权限，而不能为管理员组启用或限制数据访问权限。

默认数据访问权限

Cisco ISE 具有一系列预定义的数据访问权限。这些权限允许多名管理员在同一个用户群中具有数据访问权限。您可以启用数据访问权限或将其限制在一个或更多管理员组范围。此过程允许向一个管理员组的管理员授予自主委派控制，通过选择性关联允许所选管理员组重复使用数据访问权限。对于查看所选管理员组或网络设备组，数据访问权限范围从完全访问权限直到无访问权限。通过基于策略的管理员（RBAC）组菜单访问和数据访问权限定义。您应首先创建菜单访问和数据访问权限，然后创建将管理员组与对应菜单访问和数据访问权限关联的 RBAC 策略。RBAC 策略采用以下形式：If admin_group=Super Admin then assign SuperAdmin Menu Access permission + SuperAdmin Data Access permission。除了预定义的数据访问权限外，Cisco ISE 还允许您创建可与 RBAC 策略的自定义数据访问权限。

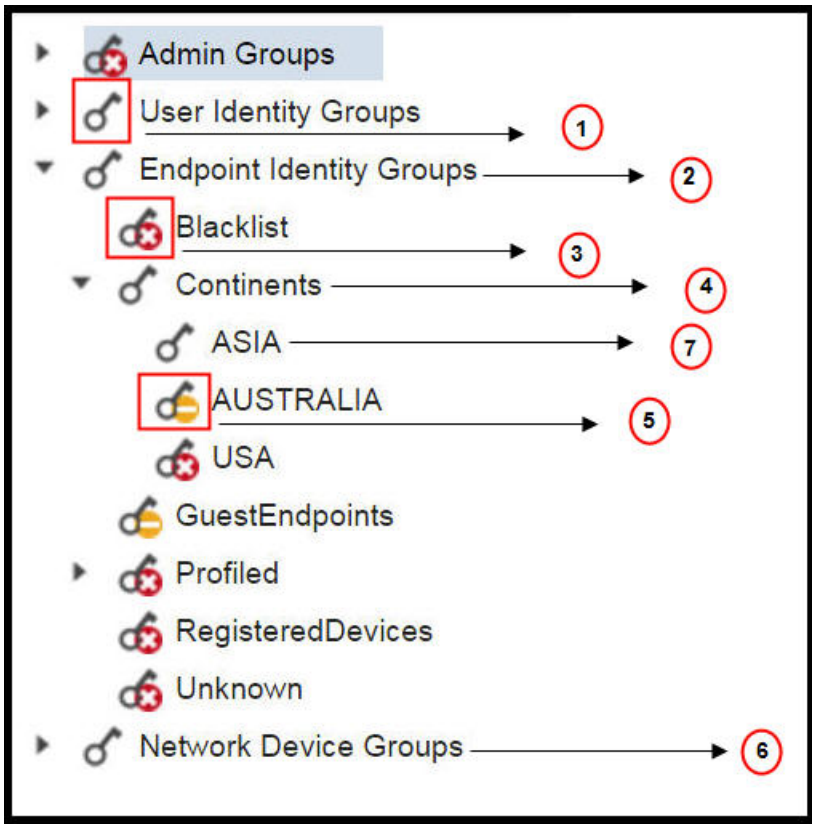
可向管理员组授予三种数据访问权限，即完全访问权限、无访问权限和只读访问权限。

只读访问权限可授予以下管理员组：

- 管理 (Administration) > 管理员访问权限 (Admin Access) > 管理员 (Administrators) > 管理员组 (Admin Groups)
- 管理 (Administration) > 组 (Groups) > 用户身份组 (User Identity Group)
- 管理 (Administration) > 组 (Groups) > 终端身份组 (Endpoint Identity Groups)
- 网络可视性 (Network Visibility) > 终端 (Endpoints)
- 管理 (Administration) > 网络资源 (Network Resources) > 网络设备组 (Network Device Groups)
- 管理 (Administration) > 网络资源 (Network Resources) > 网络设备 (Network Devices)
- Administration（管理）> Identity Management（身份管理）> Identities（身份）
- 管理 (Administration) > 身份管理 (Identity Management) > 用户身份组 (User Identity Groups)
- 管理 (Administration) > 身份管理 (Identity Management) > 终端身份组 (Endpoint Identity Groups)

如果您对某一数据类型（例如，终端身份组）具有只读访问权限，则无法对该数据类型执行 CRUD 操作。如果您对某对象具有只读访问权限（例如，GuestEndpoints），则无法对该对象执行编辑/删除操作。

图 *1:* 下图描述了如何在包含不同 ***RBAC*** 组的其他子菜单或选项的第二或第三级菜单中应用数据访问权限。



编号	说明
1	表示用户身份组数据类型的完全访问权限。
2	表示终端身份组派生授予其子项（亚洲）的最大权限（完全访问权限）。
3	表示对该对象无访问权限（阻止列表）。
4	表示父项（大洲）获得授予其子项（亚洲）的最大访问权限。
5	表示对对象的（澳大利亚）的只读访问权限。
6	表示向父项（网络设备组）授予完全访问权限时，会导致子项自动继承权限。
7	表示向父项（亚洲）授予完全访问权限时，会导致对象继承完全访问权限，除非明确授予对象权限。

配置数据访问权限

通过Cisco ISE，可以创建自定义数据访问权限，并将其映射到 RBCA 策略。根据管理员的角色，可以选择仅为他们提供选择数据的访问权限。

步骤 1 选择 **管理 (Administration)** > **系统 (System)** > **管理员访问 (Admin Access)** > **授权 (Authorization)** > **权限 (Permissions)**。

步骤 2 选择**权限 (Permissions)** > **数据访问 (Data Access)**。

步骤 3 点击**添加 (Add)**，输入**名称** 和 **说明** 字段的值。

a) 点击以展开管理员组，选择所需的管理员组。

b) 点击**完全访问 (Full Access)**、**只读权限 (Read Only Access)** 或 **不能访问 (No Access)**。

步骤 4 点击**保存 (Save)**。

只读管理员策略

默认只读管理员策略在**管理 (Administration) > 系统 (System) > 管理员访问权限 (Admin Access) > 授权 (Authorization) > RBAC 策略 (RBAC Policy)** 页面提供。此策略可用于新安装和升级部署。只读管理员策略可用于只读管理员组。默认情况下，将向只读管理员授予超级管理员菜单访问权限和只读数据访问权限。无法复制此策略，也无法编辑关联的**数据访问权限**。

注释

- 默认只读策略映射到只读管理员组。无法使用只读管理员组创建自定义 RBAC 策略。
- 思科 ISE 仅基于只读管理员组的静态检查支持只读功能。

自定义只读管理员的菜单访问权限

默认情况下，只读管理员具有超级管理员菜单访问权限和只读管理员数据访问权限。不过，如果超级管理员需要只读管理员仅查看“主页”(Home) 和“管理”(Administration) 选项卡，则超级管理员可以创建自定义菜单访问权限或自定义默认权限，例如MnT管理员菜单访问权限或策略管理员菜单访问权限。超级管理员无法修改映射到只读管理员策略的只读数据访问权限。

步骤 1 以超级管理员身份登录管理员门户。

步骤 2 导航至 **管理 (Administration) > 系统 (System) > 管理员访问 (Admin Access) > 授权 (Authorization) > 权限 (Permissions) > 菜单访问 (Menu Access)** 页面。

步骤 3 点击**添加 (Add)**，然后输入**名称**（如 MyMenu）和**说明**。

步骤 4 在**菜单访问权限 (Menu Access Privileges)** 部分中，可以选择**显示/隐藏 (Show/Hide)** 选项来选择应向只读管理员显示的所需选项（如“主页”(Home) 和“管理”(Administration) 选项卡）。

步骤 5 点击**提交 (Submit)**。

自定义菜单访问权限显示在与只读管理员策略（显示在“管理”(Administration) > “系统”(System) > “管理员访问权限权限”(Admin Access) > “授权”(Authorization) > “策略”(Policy) 页面中）对应的**权限 (Permissions)** 下拉列表中。

步骤 6 导航至**管理员 (Administration) > 系统 (System) > 管理员访问权限 (Admin Access) > 授权 (Authorization) > RBAC 策略 (RBAC Policy)** 页面。

步骤 7 点击与**只读管理员策略 (Read-Only Admin Policy)** 对应的**权限 (Permissions)** 下拉列表。

步骤 8 选择默认菜单访问权限（MnT 管理员菜单访问）或自定义菜单访问权限 (MyMenu)。 **管理 (Administration) > 系统 (System) > 管理员访问 (Admin Access) > 授权 (Authorization) > 权限 (Permissions) > 菜单访问 (Menu Access)** 页面。

步骤 9 点击**保存 (Save)**。

如果为只读管理员策略选择数据访问权限，将遇到错误。

注释 登录只读管理员门户时，屏幕顶部将显示一个只读图标，您只能查看指定的菜单选项，而没有数据访问权限。