思科 SecureX 功能区

本章概述了思科 SecureX 中的功能区，包括以下内容：

色带

思科 SecureX 是集中式控制台和分布式功能集，可统一可视性，实现自动化，加速事件响应工作流程并改善威胁搜索。这些分布式功能以 SecureX 功能区中的应用程序（应用）和工具的形式呈现。

功能区位于页面下方，当您在控制面板和环境中的其他安全产品之间移动时，此功能仍然存在。

图 *1: SecureX* 功能区 - 已折叠

使用功能区访问案例集、应用、设置、搜索用于充实的可观察对象、查看通知和查看事件。

注释 如果您是 SecureX 演示中未激活的用户，则必须单击**配置模块 (Configure a Module)** 以通过启用集成模块来激活 SecureX 帐户，然后才能访问功能区。

功能区图标和元素

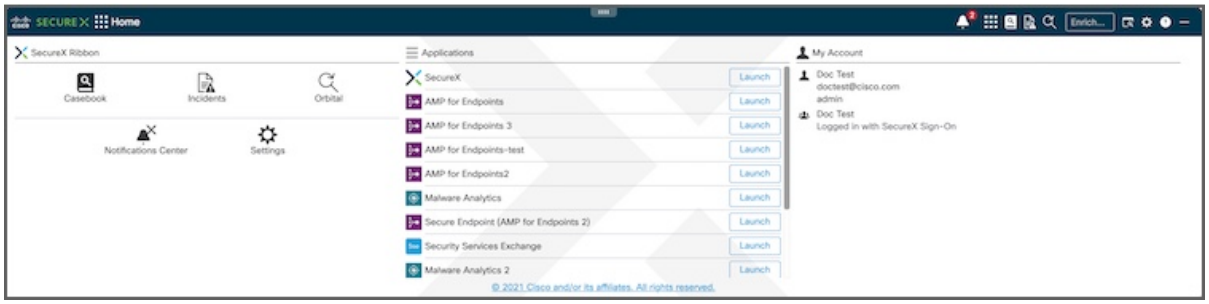
思科 SecureX 功能区上会显示以下图标和元素。

图 *2:* 功能区图标和元素

展开/折叠功能区

单击 +/- 图标以展开或折叠功能区。当功能区展开时，您可以在面板的整个顶面的任意位置上下拖动容器或在任意位置上下拖动双箭头，从而调整面板的高度。

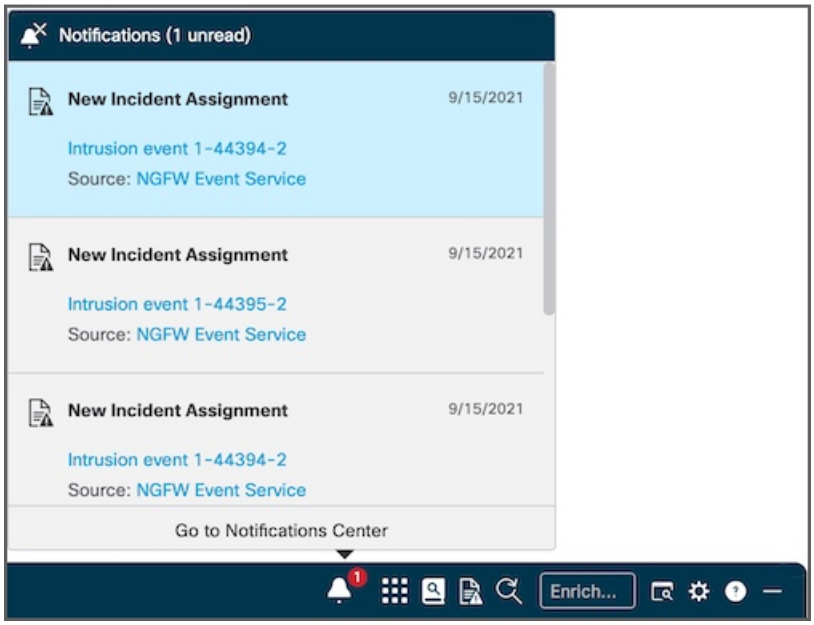
图 *3: SecureX* 功能区 - 已展开



通知

 （**通知**）图标会显示未读通知的数量。单击图标以显示其他用户在**通知 (Notifications)** 弹出窗口中分配给您的事件通知。单击图标后，未读通知会被标为已读，而未读通知的数量会重置。

图 *4:* 通知



查看通知详细信息

每个通知都包括通知类型、通知日期、可在**事件应用**中打开事件的事件标题链接，以及打开事件源的源链接（如果适用）。有关事件应用的详细信息，请参阅 SecureX 在线帮助中的**事件应用**主题。

删除通知

要删除通知，请将鼠标悬停在通知上方，然后单击**清除 (Clear)** 图标。这样也会将通知从**通知中心 (Notifications Center)** 删除。

访问通知中心

单击**转到通知中心 (Go to Notifications Center)** 链接以打开**通知中心 (Notifications Center)** 页面并管理通知。有关详细信息，请参阅 SecureX 联机帮助中的**通知中心**主题。

主页

使用功能区**主页 (Home)** 页面打开功能区应用、通知中心和功能区设置，启动集成应用，并查看帐户配置文件，其中包括用于登录的用户名、帐户邮件地址、角色、组织和 IDP。

在移至功能区中的其他页面时，单击**主页**图标可返回到功能区**主页 (Home)** 页面。

案例集应用

单击**案例手册应用**图标以打开案例手册应用并保存有关威胁分析的信息。您还可以将鼠标悬停在图标上，以查看当前案例的相关详细信息。有关详细信息，请参阅 SecureX 联机帮助中的**案例集应用**主题。

事件应用

单击**事件应用**图标以打开事件应用并查看集成产品中的事件。您还可以将鼠标悬停在图标上，以查看分配给当前案例的事件的详细信息。有关详细信息，请参阅 SecureX 联机帮助中的**事件应用**主题。

Orbital 应用

单击 **Orbital 应用**图标以打开 Orbital 应用并执行其他查询。有关详细信息，请参阅 SecureX 联机帮助中的 **Orbital 应用**主题。

增强搜索框

在**充实 (Enrichment)** 搜索框中输入搜索条件，然后按 **Enter** 开始提取可观察对象。然后，您可以单击**添加到案例 (Add to Case)** 或**在威胁响应中调查 (Investigate in Threat Response)**。有关详细信息，请参阅 SecureX 联机帮助中的**搜索可观察对象**主题。

查找可观察对象

单击**查找可观察对象 (Find Observables)** 图标，以便在当前网页中搜索恶意文件散列、可疑域和其他网络可观察对象。然后，您可以单击**将可观察对象添加到案例 (Add Observables to Case)** 或**在威胁响应中调查 (Investigate in Threat Response)**。有关详细信息，请参阅 SecureX 联机帮助。

设置

单击**设置**图标以打开 SecureX 功能区和案例集设置。

- **SecureX 功能区设置**：
  - **主题 (Theme)** - 单击选项以指定功能区的背景颜色：
    - **浅色 (Light)** - 显示浅色背景（默认）。

- **黄昏 (Dusk)** - 显示深色背景。
- **自动 (Automatic)** - 显示自动匹配集成产品主题的背景。

  当选择**自动 (Automatic)** 主题时，您还可以选择将其自动设置为**反转产品主题 (Inverse of the product theme)** 或 **匹配产品主题 (Match the product theme)**。

- **条形图格式 (Bar Format)** - 单击**完整 (Full)** 或**缩小 (Reduced)** 以设置功能区折叠时的大小。根据集成情况，此功能可能会被禁用。
- **存储 (Storage)** - 单击**清除存储 (Clear Storage)** 按钮，以便清除功能区和所有功能区应用的已存储设置和状态。这样不会删除任何数据对象，例如案例和事件。
- **版本 (Version)** - 功能区的发行版本号。
- **重置 (Reset)** - 单击**重置为默认值 (Reset to Defaults)** 按钮，以便将 SecureX 功能区的所有设置都重置为默认值。

- **案例集设置：**
  - **自动打开 (Auto Open)** - 选中此复选框可自动打开案例集中新创建的案例。此复选框会默认选中。如果您不希望在案例集中默认打开新案例，请取消选中此复选框。

    如果要在创建新案例时始终切换到案例集应用，请选中此复选框。此复选框会默认选中。如果不想在创建新案例时切换到案例集应用，请取消选中此复选框。
  - **可观察对象排序 (Observable Sort)** - 单击此选项可对案例中的可观察对象列表进行排序：
    - **最新 (Newest)** - 按可观察对象被添加到案例中的顺序来显示可观察对象的列表（从最新到最旧）。
    - **最旧 (Oldest)** - 按可观察对象被添加到案例中的顺序来显示可观察对象的列表（从最旧到最新）。
    - **字母顺序 (Alphabetical)** - 按字母顺序显示可观察对象列表（从 A 到 Z）。
  - **重置 (Reset)** - 单击**重置为默认值 (Reset to Defaults)** 按钮可将案例集应用的所有设置重置为默认值。

- **通知中心设置：**
  - **请勿打扰 (Do Not Disturb)** - 单击可启用或禁用传入通知以及**通知**图标上显示的未读通知数量。切换开关默认为禁用（关闭）；如要启用此选项，请通过切换为开来启用**请勿打扰 (Do Not Disturb)**。
  - **重置 (Reset)** - 单击**重置为默认值 (Reset to Defaults)** 按钮以将通知中心的设置重置为默认值。

帮助

单击 SecureX 功能区上的**帮助**图标，以便打开 SecureX 在线帮助中的功能区主题，了解有关功能和应用的更多信息。