安全

通过IP范围限制Alma登录

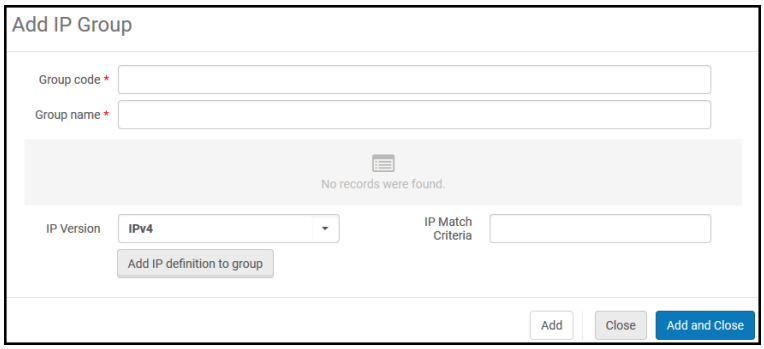
要配置IP组配置，您必须具有以下角色：

- 通用系统管理员

您可以根据IP地址限制用户登录到Alma。配置此功能有两步。首先创建IP组，然后为这些组配置登录权限。只有这些IP组能登录Alma。

使用IP组限制登录：

1. 在IP组配置页面（**配置菜单> 通用> 安全> IP组配置**），点击**添加IP组**。出现"添加IP组"。

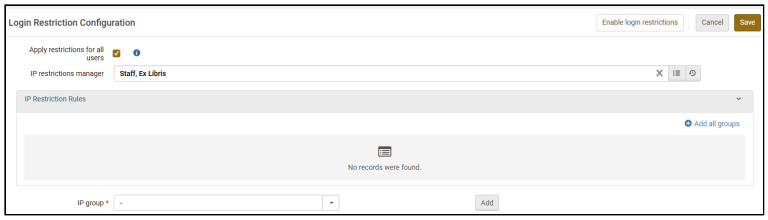


添加 IP 组

2. 输入下列信息：
   - 组代码 – IP 组代码
   - 组名 – 可以稍后更改的IP组的名称
   - IP版本 – IPv4 or IPv6
   - IP匹配标准 - 特定IP地址或IP范围（两个有效IP地址用连字符分隔）
3. 选择**添加 IP 定义到组**。该范围将添加到组中，并显示在表中。
4. 您可以为每个组定义多个IP范围。按需重复步骤2和3。要删除IP范围，点击**删除**。
5. 完成添加后，点击 **添加和关闭**。IP组已添加。

   要编辑IP组，点击**编辑**。要删除组，点击**删除**。

6. 打开登录限制配置页面（**配置菜单> 通用> 安全> 登录限制配置**）。请注意，您在此页启用前登录限制都是停用状态。



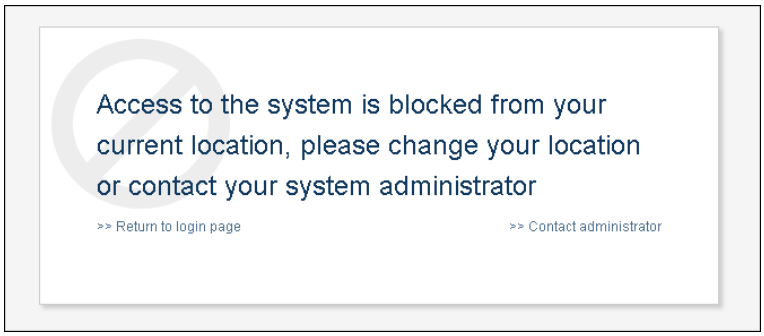
登录限制配置

7. 可以通过在编辑用户时选择**禁用所有登录限制**（见编辑用户）来针对特定用户覆盖登录限制。
（五月新增）选择**对所有用户应用限制**复选框取消用户级别覆盖并对具有通用系统管理员角色的用户应用登录限制。请注意，之前的配置不会被删除，一旦取消选中复选框，它就会恢复。
8. 从**IP组**中选择要允许登录访问的IP地址的IP组，点击**添加**。 您可以点击**添加所有组**以添加所有IP组。
一旦选定了IP组，其他的IP地址都会被限制登录。
9. 从**IP限制管理器**框中选择一个管理员（必填）。当用户使用受限的IP地址进行登录尝试时，该管理员会收到所有相关信息。
10. 选择**启用登录限制**。要保存更改而不启用或禁用登录限制，点击**保存**。

Note

- 您必须点击**启用登录限制**才能使IP登录限制生效。
- 具有通用系统管理员角色的用户不受限制。
- 要在以后禁用登录限制，点击 **禁用登录限制**。

如果有用户使用受限IP地址尝试登录Alma，则会显示以下消息：

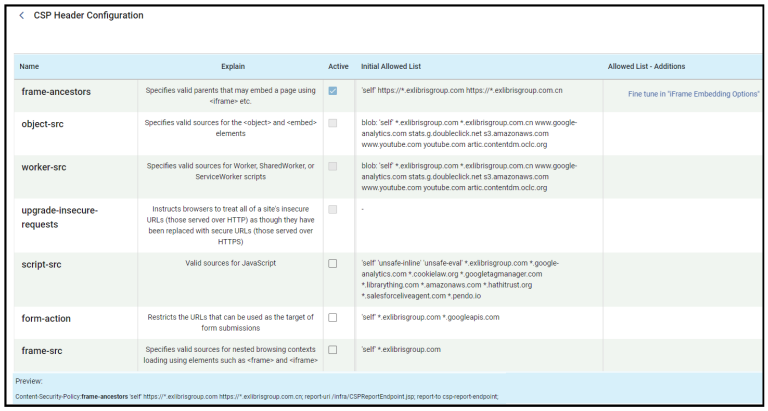


访问已被阻止

用户可以点击**联系管理员**联系之前配置的IP限制管理员。

CSP（内容安全政策）标头配置

您可以启用和配置CSP标头指令来微调Web应用程序的安全政策。要访问此配置，请转到**配置 > 通用 > CSP标头配置**。



CSP标题配置

底部的预览窗格显示标头，并在设置更改时自动更新。

前四条指令（frame-ancestors、object-src、worker-src、upgrade-insecure-requests）默认处于有效状态，并且无法禁用。然而，您可以在**允许列表 - 添加**列中将其他域添加到允许列表。

最后五条指令（如下所述）默认处于停用状态，但与前四个指令不同，它们可以激活。您可以在**允许列表 - 添加**列中将其他域添加到允许列表。

1. **form-action**:
   - 此指令限制可用作表单提交目标的URL（`<form action="..." />`）。它有助于防止表单被提交到恶意网站。
2. **base-uri**：
   - 此指令限制可以在文档的`<base>`元素中使用的URL。`<base>`元素指定用于文档中所有相对URL的基础URL，因此控制此元素可防止攻击者更改基础URL并将链接重定向到恶意网站。
3. **script-src**：
   - 此指令指定JavaScript的有效来源。它仅允许来自可信来源的脚本在页面上执行，从而有助于减轻XSS攻击。例如，您可以指定仅从自己的域或受信任的CDN加载脚本。
4. **frame-src**：
   - 该指令指定使用`<frame>`、`<iframe>`、`<object>`、`<embed>`和`<applet>`嵌入内容的有效来源。它有助于控制哪些源可以嵌入框架内，从而防止点击劫持和其他类型的框架式攻击。
5. **connect-src**：
   - 该指令使用诸如`XMLHttpRequest`、`Fetch`、`WebSocket`和EventSource的机制来限制文档可以获取的URL。它有助于控制脚本可以发送数据的位置，从而降低数据泄露的风险。
6. **style-src**：
   - HTTP `Content-Security-Policy` (CSP) `style-src`指令指定样式表的有效来源。
7. **img-src**：
   - HTTP `Content-Security-Policy` `img-src`指令指定图像和图标的有效来源。
8. **font-src**：

- HTTP `Content-Security-Policy` (CSP) `font-src` 指令指定使用 `@font-face` 加载的字体的有效来源。

9. **child-src**：
   - HTTP `Content-Security-Policy` (CSP) `child-src` 指令定义使用 `<frame>` 和 `<iframe>` 等元素加载的Web工作线程和嵌套浏览上下文的有效来源。对于工作线程来说，不合规的请求会被用户代理视为致命的网络错误。
10. **default-src**：
    - HTTP `Content-Security-Policy` (CSP) `default-src` 指令可作为其他CSP获取指令的备用方法。对于每个缺失的指令，用户代理都会查找 `default-src` 指令并使用该值。

登录重定向允许列表

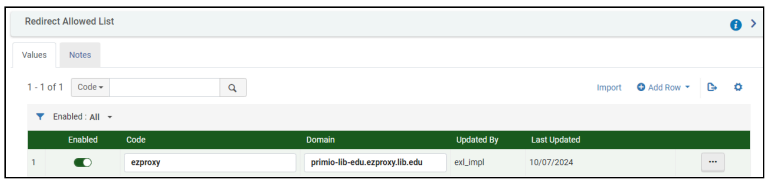
为了避免潜在的安全问题（开放重定向漏洞），您可以创建受信任站点列表。

要创建受信任站点列表：

1. 确保**limit_login_redirects**（**配置 > 通用 > 其他设置**）参数设置为true。
2. 导航到**配置 > 通用 > 重定向允许列表**。
3. 为每个受信任域添加一个新行。该代码仅供描述之用，并非由Alma使用。

Note

属于Ex Libris (*.exlibrisgroup.com)的域名无需列出。



防止点击劫持

要控制iFrame嵌入选项，您需要有以下角色：

- 通用系统管理员

点击劫持是通过显示含有敏感页面的实际控制的无害页面欺骗用户的攻击。这些控制通过使用背景框架掩盖，用户无法识别他们是否在网站上点击了敏感功能。这可以导致用户无意中下载恶意软件并提供密码等敏感信息、转账或者在线购物。

为了防止来自ExLibris产品的点击劫持，ExLibris使用基于政策的缓和技术。现在机构的站点如果包含在iframe中，可以指示浏览器执行合适的操作。

Note

修改该页面可能会损害其他产品的界面集成。如果对于如何使用该页面有疑问，联系Ex Libris客户支持。

要设置如果站点包含在iframe中执行的操作：

1. 打开**iFrame嵌入选项**表（**配置 > 通用 > 安全 > iFrame嵌入选项**）。
2. 对需要的产品和组件，选择**自定义**。

Note

- Alma管理和Esploro管理无法修饰。该配置无法编辑。
- 如果您使用Azure IDP，则不支持IFrame嵌入。

3. 在**操作**栏中，选择您的站点包含在iFrame中时执行的操作：
   - **允许所有**（默认选项） — 允许所有页面在iFrame中加载该页面。
   - **允许保护的** — 仅信任允许在iFrame中加载该页面的页面。如果选择该选项，在**安全域名**栏指示信任的URL（URL的数量不限，多个URL以空格分隔）。

Note

我们建议添加https://*.WEBSITEHERE.com，例如，https://*.amazon.com”。

   - **限制全部** — 拒绝所有修饰页面的尝试。
4. 选择**保存**。