

Cisco WAP121和WAP321接入点上的密码复杂性配置

目标

密码复杂性的增加降低了安全漏洞的风险。黑客通常可以在几小时内破解长度小于8个字符的密码。因此，使用长密码时必须同时使用大小写字母、数字和符号。

本文介绍WAP121和WAP321接入点上的密码复杂性配置。

适用设备

- WAP121
- WAP321

软件版本

- 1.0.3.4

密码复杂性配置

步骤1.登录Web配置实用程序，然后选择System Security > Password Complexity。“密码复杂性”页面打开：

Password Complexity

Password Complexity: Enable

Password Minimum Character Class: 3

Password Different From Current: Enable

Maximum Password Length: 64 (Range: 64 - 80, Default: 64)

Minimum Password Length: 8 (Range: 0 - 32, Default: 8)

Password Aging Support: Enable

Password Aging Time: 180 Days (Range: 1 - 365, Default: 180)

Save

Password Complexity:	<input checked="" type="checkbox"/> Enable
Password Minimum Character Class:	3
Password Different From Current:	<input checked="" type="checkbox"/> Enable
Maximum Password Length:	72 (Range: 64 - 80, Default: 64)
Minimum Password Length:	16 (Range: 0 - 32, Default: 8)
<hr/>	
Password Aging Support:	<input checked="" type="checkbox"/> Enable
Password Aging Time:	100 Days (Range: 1 - 365, Default: 180)

步骤2.在Password Complexity字段中选中**Enable**以启用密码复杂性。

步骤3.从密码最小字符类下拉列表中选择适当的最小字符类数。大写字母、小写字母、数字和标准键盘上可用的特殊字符是四种可能的字符类。

第4步。(可选)在“密码与当前密码不同”字段中选中**启用**，以要求在当前密码到期时输入不同的密码。如果禁用，您可以重新输入之前使用的相同密码。

步骤5.在Maximum Password Length字段中输入密码的最大字符数。范围从 64 至 80。

步骤6.在Minimum Password Length字段中输入密码可以具有的最小字符数。范围从 0 至 32。

Password Aging Support:	<input checked="" type="checkbox"/> Enable
Password Aging Time:	100 Days (Range: 1 - 365, Default: 180)

第7步。(可选)在Password Aging Support字段中选中**Enable**，使密码在特定时间后过期。

步骤8.如果在上一步中启用了密码老化支持，请在Password Aging Time字段中输入密码过期前的天数。范围为1至365天。

第 9 步： 点击 **Save (保存)**，以保存设置。