

在300系列被管理的交换机的SNTP认证

客观

Simple Network Time Protocol (SNTP)是使用同步在互联网的计算机时钟网络时间协议 (NTP)的适应。对一起是连网有同步的时间的设备是重要，因此他们可彼此高效地进行实时动作。要执行此，必须添加Sntp server到交换机，并且必须配置SNTP认证密钥。认证密钥允许设备与Sntp server同步自己。

关于如何添加Sntp server的更多信息请参见条款添加在300系列被管理的交换机的一Sntp server。

此条款说明如何配置在300系列被管理的交换机的SNTP认证。

可适用的设备

- SG300-10PP
- SG300-10MPP
- SG300-28PP-R
- SG300-28SFP-R
- SF302-08MPP
- SF302-08PP
- SF300-24PP-R
- SF300-48PP-R

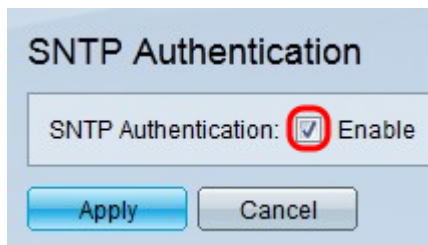
软件版本

- 1.4.0.00p3 [SG300-28SFP-R]
- 6.2.10.18 [All other Applicable Devices]

SNTP认证

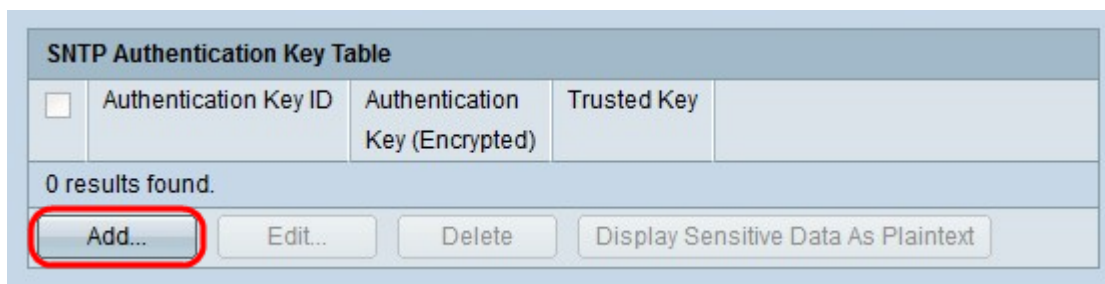
步骤1. 登录到Web配置工具并且选择Administration > 时间设定 > SNTP认证。SNTP认证页打开：

Authentication Key ID	Authentication Key (Encrypted)	Trusted Key
0 results found.		

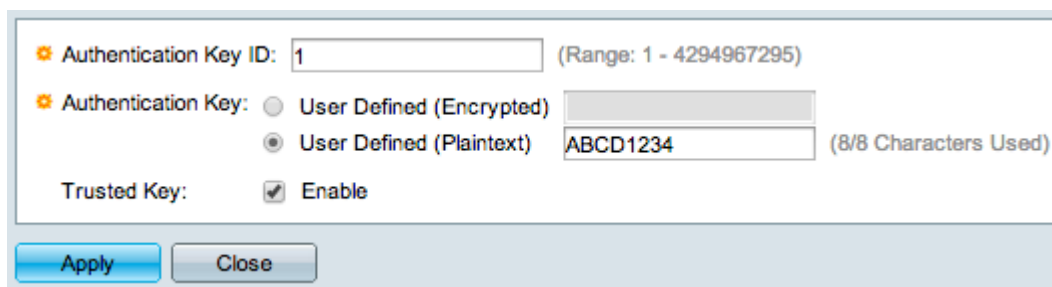


Step 2.检查在SNTP认证字段的**Enable复选框**要求一次SNTP会话的认证在交换机和Sntp server之间的。

步骤3.点击**适用**。



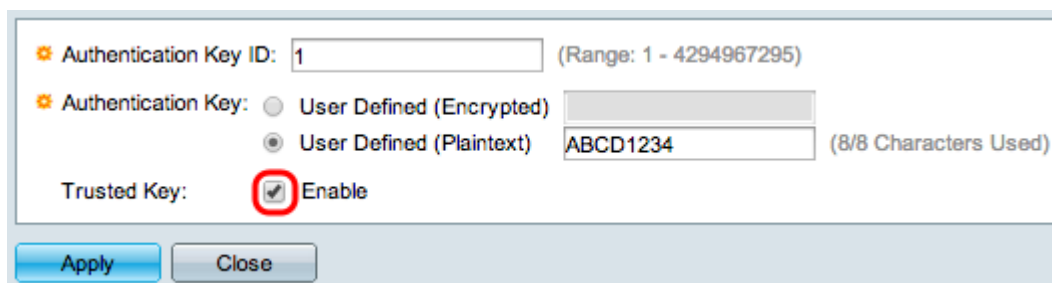
步骤4.点击**添加**添加认证密钥。**添加SNTP认证**窗口出现。



步骤5.输入使用识别SNTP认证密钥内部地在认证密钥ID字段的编号。

步骤6.点击对应于期望关键输入认证密钥领域的单选按钮。Sntp server必须发送交换机的此键能同步到它。

- 用户定义(加密) —输入键在被加密的格式。
- 用户定义(明文) —输入键在无格式文本格式。



第 7 步：检查在信任键关键字域的**Enable复选框**允许交换机从仅Sntp server获得使用被定义的认证密钥的同步信息。

步骤8.点击**适用**。配置SNTP认证密钥。

SNTP Authentication Key Table			
<input checked="" type="checkbox"/>	Authentication Key ID	Authentication Key (Encrypted)	Trusted Key
<input checked="" type="checkbox"/>	1	OcosVc2HLdR7Ma...	Enabled

第9步(可选)编辑SNTP认证密钥检查您希望编辑并且点击**编辑**STNP认证的复选框。 *Edit*页打开。

Authentication Key ID:

Authentication Key: User Defined (Encrypted)

User Defined (Plaintext) (0/8 Characters Used)

Trusted Key: Enable

第10步(可选)编辑您要配置的设置。SNTP将发送交换机的认证密钥能同步到它。

- 用户定义(加密) — 输入键在被加密的格式。
- 用户定义(明文) — 输入键在无格式文本格式。
- 信任键—非选定将禁用交换机从仅Sntp server获得同步信息使用被定义的认证密钥的 enable (event) 机箱

第11步(可选)删除SNTP认证密钥，检查您希望删除并且点击**删除**SNTP认证密钥的复选框。

SNTP Authentication Key Table			
<input checked="" type="checkbox"/>	Authentication Key ID	Authentication Key (Encrypted)	Trusted Key
<input checked="" type="checkbox"/>	1	OcosVc2HLdR7Ma...	Enabled