TOTP 令牌（动态令牌）配置举例

目 录

1 简介

TOTP 是基于时间的一次性密码算法的简称。这个算法通过一个共享密钥和当前时间来计算一次性密码。经常被用于双因素认证的系统中。因为网络延时或者时钟没有完全同步的原因，一般生成一次密码，需要 60 秒的发送间隔。

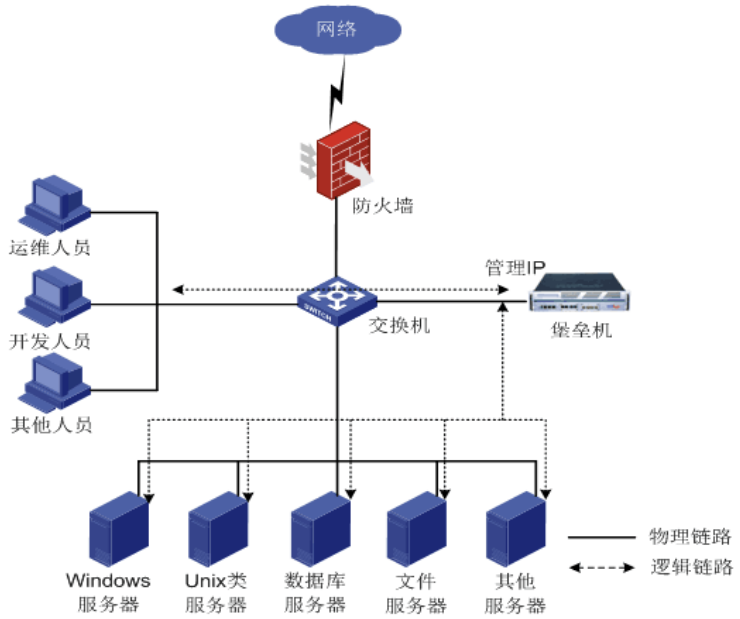
2 配置前提

因为 TOTP 令牌与时间密切相关，所以在配置 TOTP 令牌前，请确保运维审计系统的时间与北京时间一致。

3 配置举例

3.1 组网需求

图3-1 TOTP 令牌认证网络图



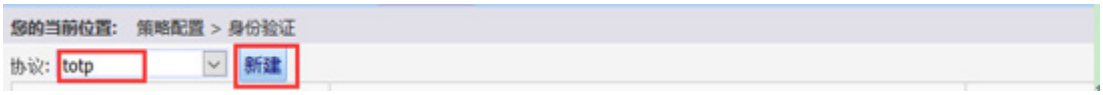
3.2 系统版本要求

适用产品版本：ESS 6101 及以上版本。

3.3 新建TOTP认证方式

(1) 超级管理员，“策略配置 > 身份验证”，选择“totp”，点击“新建”。

图3-2 新建 TOTP 认证方式



(2) 修改属性

- 状态：选择为启用。
- 名称：填写此 totp 名称。

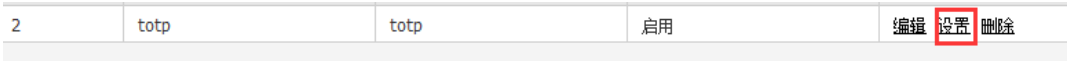
点击确定。

图3-3 修改属性

3.4 TOTP令牌管理

点击“设置”。

图3-4 TOTP 令牌管理



3.4.1 单个令牌管理

1. 导入令牌

(1) 点击“新建”。

图3-5 导入令牌

(2) 输入对应的 key 和 SN 号码，点击“确定”。

图3-6 输入对应的 key 和 SN 号码

注：图中 key 值前面两位是小写的字母 l，不是数字 1

2. 令牌同步

方法一：

(1) 当令牌使用一段时间之后，可能由于时钟漂移，导致一次性密码产生错误，这时需要同步令牌。选择相应令牌，点击“同步”。

图3-7 同步令牌

(2) 将令牌产生的两个一次性密码，依次填入“密码 1”、“密码 2”。点击“同步”。

图3-8 输入密码

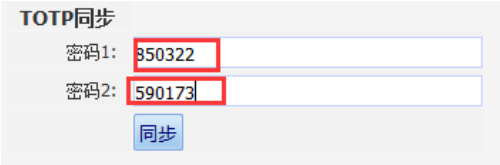
方法二：

(1) 页面右上角，进入“账户设置”

图3-9 账户设置

(2) 将令牌产生的两个一次性密码，依次填入“密码 1”、“密码 2”。点击“同步”。

图3-10 输入密码

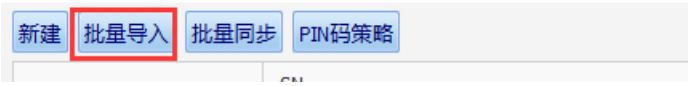


3.4.2 批量令牌管理

1. 批量导入令牌

(1) 点击“批量导入”。

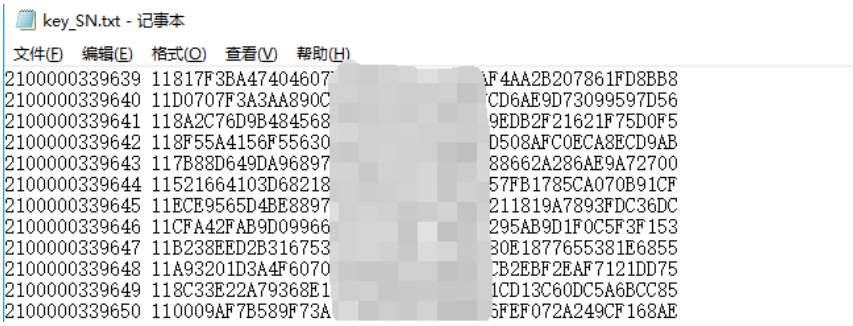
图3-11 批量导入令牌



(2) 将 key 和 SN 号写入文本。

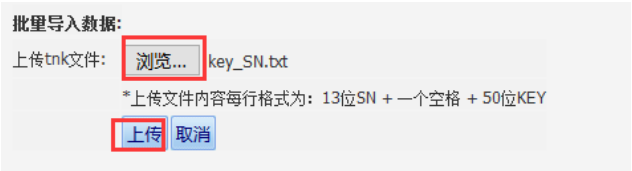
格式：13 位 SN + 一个空格 + 50 位 KEY。

图3-12 将 key 和 SN 号写入文本



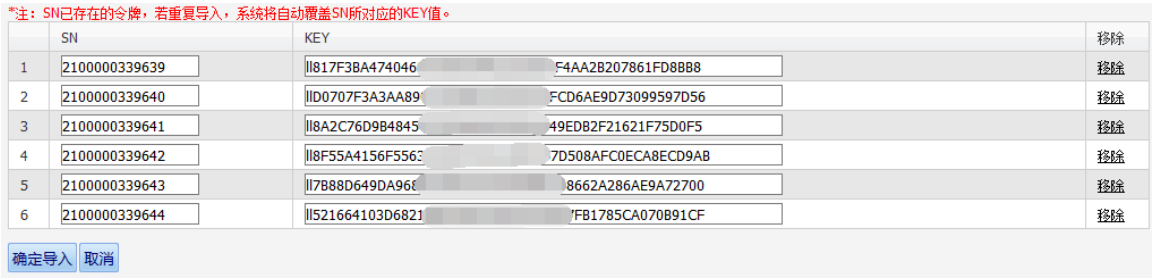
(3) 导入该文本。

图3-13 导入文本



(4) 点击“确定导入”。

图3-14 确认



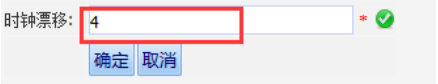
2. 批量同步令牌

(1) 点击“批量同步”。

图3-15 批量同步令牌

(2) 设置时钟漂移，然后点击确定。

图3-16 设置时钟漂移



3.4.3 PIN码策略

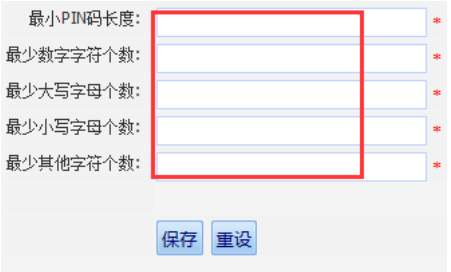
TOTP 令牌不能单独作为验证工具，必须与另外的静态密码进行绑定，我们在运维审计系统中，将这个静态密码称为 PIN 码。

点击“PIN 码策略”。

图3-17 PIN 码策略

设置需要的 PIN 码复杂度。

图3-18 设置 PIN 码复杂度



3.5 创建用户，绑定TOTP令牌

“基本控制 > 用户账号 > 新建用户”。

图3-19 创建用户

- 登录名：登录运维审计系统的账户名。
- 真实姓名：该账户名的真实用户。
- 部门：选择相应的部门。
- 身份验证方式：这里选择之前配置的 totp。
- SN：选择需要绑定的令牌 SN（一个令牌最多可以分配给 5 个用户使用）。
- PIN1：用户登录时使用的静态密码。
- PIN2：用户做双人授权时使用的静态密码。

图3-20 配置用户信息

3.6 TOTP使用

3.6.1 TOTP登录

输入账户、密码。

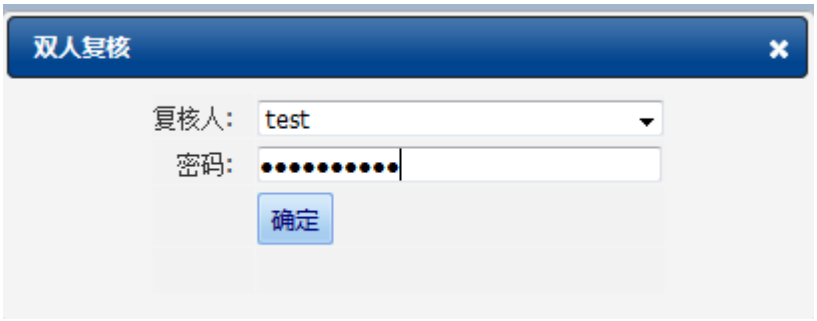
密码格式为：PIN1 码+令牌数字

图3-21 TOTP 登录

3.6.2 TOTP双人复核

密码：输入 PIN2 码+令牌。

图3-22 TOTP 双人复核



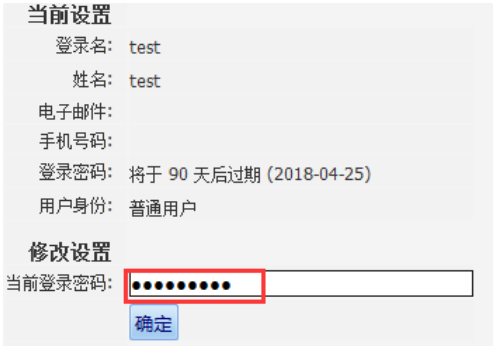
3.6.3 TOTP修改PIN1、PIN2 码

(1) 页面右上角，进入“账户设置”

图3-23 账户设置

(2) 输入：PIN1 码+令牌

图3-24 PIN1 码+令牌



(3) 切换到“自由修改密码”，修改 PIN1、PIN2 码。

图3-25 修改 PIN1、PIN2 码