

TOTP 令牌（动态令牌）配置举例

Copyright © 2018 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。

目 录

1 简介	1
2 配置前提	1
3 配置举例	1
3.1 组网需求	1
3.2 系统版本要求	1
3.3 新建TOTP认证方式	2
3.4 TOTP令牌管理	2
3.4.1 单个令牌管理	2
3.4.2 批量令牌管理	4
3.4.3 PIN码策略	5
3.5 创建用户，绑定TOTP令牌	6
3.6 TOTP使用	6
3.6.1 TOTP登录	6
3.6.2 TOTP双人复核	7
3.6.3 TOTP修改PIN1、PIN2 码	7

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。

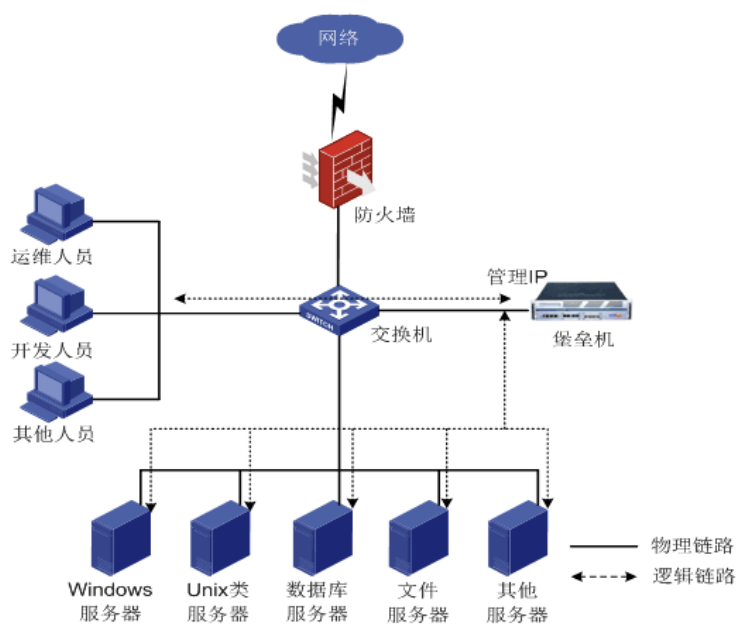
2 配置前提

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

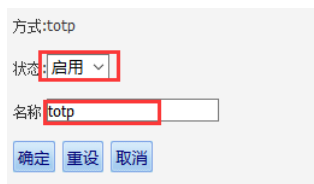


(2) 修改属性

- 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

2	totp	totp	启用	编辑 设置 删除
---	------	------	----	----------

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

SN: 2100000259874 * ✓
KEY: 110BEA0B5777CE72A12DA2A8FDE17 * ✓
确定 取消

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

	SN	归属人	时钟漂移	动作
1	2100000259874		0	编辑 同步 删除

(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

TOTP令牌同步
SN: 2100000259874
密码1: 740312
密码2: 051872
同步 取消

方法二：

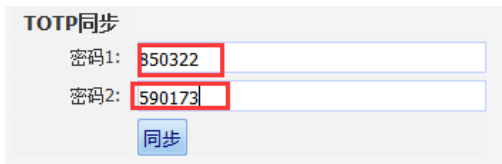
(1) 页面右上角，进入“账户设置”

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



TOTP同步

密码1: 350322

密码2: 590173

同步

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

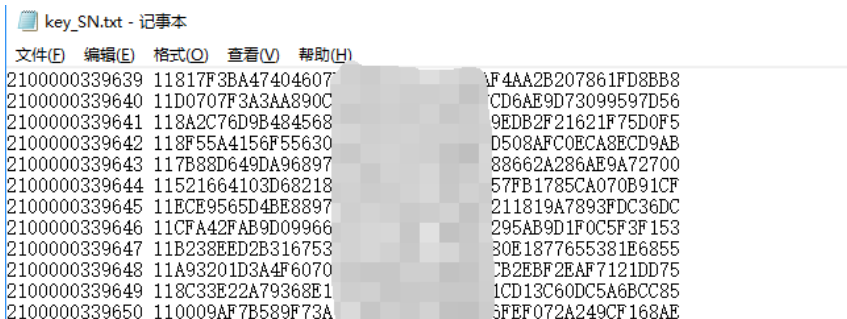


新建 批量导入 批量同步 PIN码策略

(2) 将 key 和 SN 号写入文本。

格式：13 位 SN + 一个空格 + 50 位 KEY。

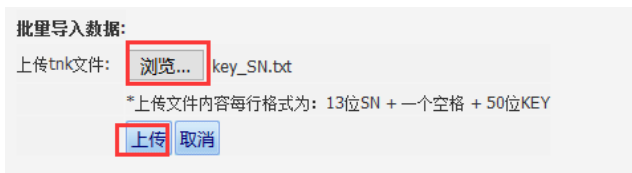
图3-12 将 key 和 SN 号写入文本



```
key_SN.txt - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
2100000339639 11817F3BA47404607 1F4AA2B207861FD8BB8
2100000339640 11D0707F3A3AA890C CD6AE9D73099597D56
2100000339641 118A2C76D9B484568 9EDB2F21621F75D0F5
2100000339642 118F55A4156F55630 D508AFC0ECA8ECD9AB
2100000339643 117B88D649DA96897 88662A286AE9A72700
2100000339644 11521664103D68218 57FB1785CA070B91CF
2100000339645 11ECE9565D4BE8897 211819A7893FDC36DC
2100000339646 11CFA42FAB9D09966 295AB9D1F0C5F3F153
2100000339647 11B238EED2B316753 30E1877655381E6855
2100000339648 11A93201D3A4F6070 CB2EBF2EAF7121DD75
2100000339649 118C33E22A79368E1 1CD13C60DC5A6BCC85
2100000339650 110009AF7B589F73A 5FEF072A249CF168AE
```

(3) 导入该文本。

图3-13 导入文本



批量导入数据:

上传tnk文件: 浏览... key_SN.txt

*上传文件内容每行格式为: 13位SN + 一个空格 + 50位KEY

上传 取消

(4) 点击“确定导入”。

图3-14 确认

*注：SN已存在的令牌，若重复导入，系统将自动覆盖SN所对应的KEY值。

	SN	KEY	移除
1	2100000339639	817F38A474046 F4AA2B207861FD88B8	移除
2	2100000339640	D0707F3A3AA89 FCD6AE9D73099597D56	移除
3	2100000339641	8A2C76D9B4845 49ED82F21621F75D0F5	移除
4	2100000339642	8F55A4156F5563 7D508AFC0ECA8ECD9AB	移除
5	2100000339643	7B88D649DA96E 8662A286AE9A72700	移除
6	2100000339644	521664103D6821 FB1785CA070B91CF	移除

确定导入 取消

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

时钟漂移: * ✓

确定 取消

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

最小PIN码长度: *

最少数字字符个数: *

最少大写字母个数: *

最少小写字母个数: *

最少其他字符个数: *

保存 重设

3.5 创建用户，绑定TOTP令牌

“基本控制 > 用户帐号 > 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

状态：禁用 活动 (查看登录日志 查看可登录设备 分配用户组 管理访问规则 用户帐号设置)

登录名： *

真实姓名： *

邮件地址：

手机号码：

部门： *

职位：

工号：

身份验证方式：

SN： *

PIN1：

PIN2：

下次登录时须修改PIN码

权限： 超级管理员 审计管理员 配置管理员 密码保管员 普通用户

审计权限： 下载会话 键盘事件
(需要下载会话权限，必须勾选键盘事件权限)

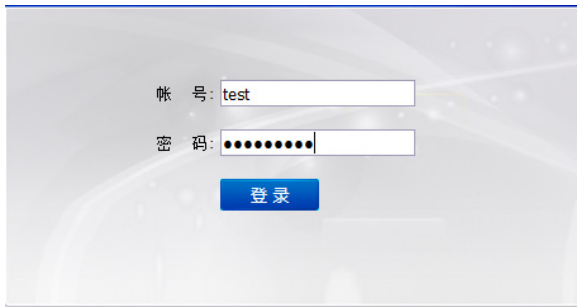
3.6 TOTP使用

3.6.1 TOTP登录

输入账户、密码。

密码格式为：PIN1 码+令牌数字

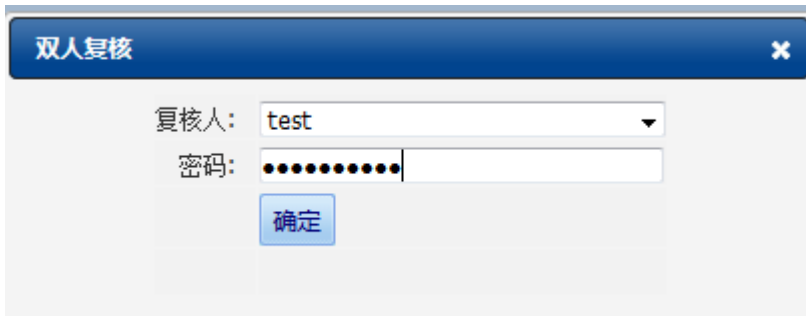
图3-21 TOTP 登录



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

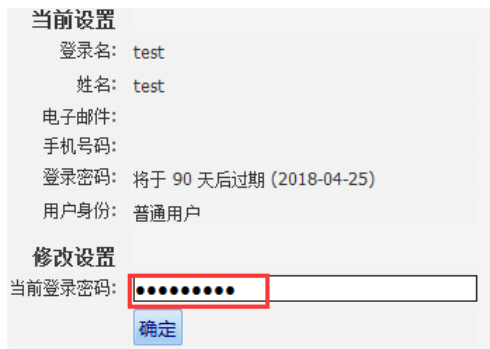
(1) 页面右上角，进入“账户设置”

图3-23 账户设置



(2) 输入：PIN1 码+令牌

图3-24 PIN1 码+令牌



当前设置

登录名: test
姓名: test
电子邮件:
手机号码:
登录密码: 将于 90 天后过期 (2018-04-25)
用户身份: 普通用户

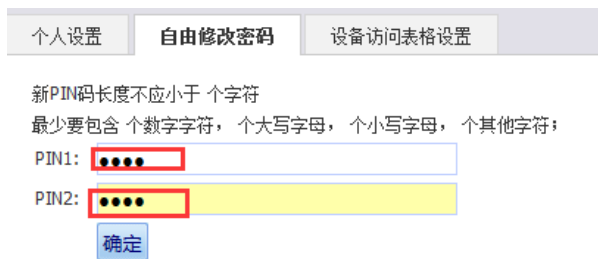
修改设置

当前登录密码:

确定

(3) 切换到“自由修改密码”，修改 PIN1、PIN2 码。

图3-25 修改 PIN1、PIN2 码



个人设置 **自由修改密码** 设备访问表格设置

新PIN码长度不应小于 个字符
最少要包含 个数字字符， 个大写字母， 个小写字母， 个其他字符：

PIN1:

PIN2:

确定