PINsafe Configuration Best Practices

Contents

Overview

Each Swivel installation will have its own requirements that will require changes to standard configurations. However below are some best practices for configuring Swivel policies and settings.

Policy>General

- Security String Type: Numbers, Upper Case Letters, Lower Case Letters, Mixed numbers and letters

Default: Numbers

Best Practice: Numbers or Upper Case Letters

- Account lockout time (minutes):

Default: 0

Best Practice: 30 minutes

- Maximum login tries: 0-99

Default: 5

Best Practice: Testing 0 (no lockout), Initial provisioning: 5, Long Term production: 3

- Increment Login failure count if user has no security strings: Yes/No

Default: Yes

Best Practice: Yes

- Inactive account expiry (days):

Default 0 (no expiry)

Best Practice: 90

- Auto. set credentials on user creation: Yes/No

Default: Yes

Best Practice: Yes

Policy>PIN and OTC

- PIN expiry (days): 0-99

Default: 0 (no expiry)

Best Practice: as PIN expiry (where change PIN is available)

- PIN expiry after auto/admin reset (days): 0-99

Default: 0

Best Practice: Yes (where change PIN is available)

- PIN expiry warning (days): 0-99

Default: 0 (no expiry)

Best Practice: 14

- Auto-reset PIN on expiry: Yes/No

Default: No

Best Practice: Yes

- PIN change grace period (days): 0-99

Default: 0

Best Practice: 7

- Require PIN change after auto. setting:

Default: No

Best Practice: Yes (where change PIN is available)

- Require PIN change after admin. reset:

Default: No

Best Practice: Yes (where change PIN is available)

- Require password for PIN change: Yes/No

Default: Yes

Best Practice: Yes (where change PIN is available)

- Only warn user, do not lock account: Yes/No

Default: No

Best Practice: No, (Yes if Auto-reset PIN on expiry is used)

- Minimum PIN size: 4-10

Default: 4

Best Practice: 4

- PINless OTC length: 4-10

Default: 6

Best Practice: 6

- Maximum repeated PIN digits:

Default: 0 (digits may not be repeated)

Best Practice: 0

- Allow numerical sequences for PIN:

Default: Yes

Best Practice: No

Policy>Password

- Require password:

Default: No

Best Practice: No (Where another primary/secondary authentication server is used in access device)

Policy>Self-Reset

- Allow user self-reset: Yes/No

Default: No

Best Practice: Yes

- Send reset code as security string: Yes/No

Default: No

Best Practice: No

- Maximum self-reset tries: 0-99

Default: 3

Best Practice: 3

- Allow user self-provision of mobile client: Yes/No

Default: No

Best Practice: Yes

- Send provision code as security string: Yes/No

Default: No

Best Practice: No

- Log device information when provisioning: Yes/No

Default: No

Best Practice: Yes

- Provision Code Validity period (seconds): 10-1000000

Default: 600

Best Practice: 86400

Policy>Helpdesk

- Helpdesk Users can manage other repositories: Yes/No

Default: No

Best Practice: No

- Helpdesk can reset PINs: Yes/No

Default: Yes

Best Practice: No

- Helpdesk Users can administer editable repositories: Yes/No

Default: No

Best Practice: No

- Helpdesk can view Status page: Yes/No

Default: Yes

Best Practice: Yes

- Helpdesk can view Log Viewer page: Yes/No

Default: Yes

Best Practice: No

- Helpdesk can view reports:

Default: No

Best Practice: No

Policy>Console Login

- Show the password field: Yes/No

Default: Yes

Best Practice: No

- Use single channel login: Yes/No

Default: Yes

Best Practice: Yes

- Update TURing immediately after entering username: Yes/No

Default: No

Best Practice: Yes

Policy>Banned Credentials

Default: None

Best Practice: 19??, 200?, 201?

Policy>Mobile Client

- Allow user to enter PIN: Yes/No

Default: No

Best Practice: No

- Allow user to choose how to extract OTC: Yes/No

Default: No

Best Practice: No

- Allow user to browse strings: Yes/No

Default: No

Best Practice: No

Logging>SMTP

- Send errors:

Default: No

Best Practice: No (where Syslog is used)

- Send account locks:

Default: No

Best Practice: Yes

- Send User Account Create/Delete:

Default: No

Best Practice: No

Transport>User Alerts

- PIN changed: Yes/No

Default: Yes

Best Practice: Yes

- PIN change required: Yes/No

Default: Yes

Best Practice: Yes

- PIN expiry warning: Yes/No

Default: Yes

Best Practice: Yes

- Account locked: Yes/No

Default: Yes

Best Practice: Yes

- Account unlocked: Yes/No

Default: Yes

Best Practice: Yes

- Account inactive: Yes/No

Default: Yes

Best Practice: Yes

- Device key allocated: Yes/No

Default: Yes

Best Practice: Yes

- No transport is error: Yes/No

Default: No

Best Practice: No

Database>General

- Case sensitive usernames: Yes/No

Default: No

Best Practice: No

Server Agents and RADIUS NAS

- Check password with Repository:

Default: No

Best Practice: No (Where another primary/secondary authentication server is used in access device)