Database Schema

Contents

Introduction

This technical document describes the schema for the Swivel Server database. It is provided for technically-competent customers who wish to access the database directly to generate reports not available elsewhere. For examples of scripts which can be used to query PINsafe, see MySQL Queries How To Guide.

IMPORTANT: Swivel Secure does not support using this information to modify the database directly, unless explicitly instructed by Swivel technical staff. Swivel Secure accept no responsibility for problems caused by modifying the database directly without supervision. This information is provided for read-only access.

NOTE: the Internal database is encrypted, and is also restricted to a single connection, so you cannot access it directly. You can export a snapshot of the current database to an external source using the Migrate option from the administration console.

Database Schema

Explanation of Tables

All the database tables are named as "PINSAFE*X*", where *X* is a single letter A, B, etc. All database fields have single character names, A, B, etc.

Tables are listed below, each in its own section. The section title describes the table usage. The table name is listed next, followed by a list of fields with their descriptions.

Note on table availability: The table naming convention listed below dates from version 3.2 onwards. Versions of PINsafe prior to 3.2 have a completely different naming convention. Unless otherwise stated, the tables are available in all versions of PINsafe from 3.2 (but see notes on Activities table).

Users

Table Name: PINSAFEJ

This is the main users table, containing one record for each user.

Fields

- *G* - The user ID. This is used to reference the user in other tables. It is generated automatically by Swivel.
- *H* - Username. As read from the repository.
- *C* - Lower-case username. Used internally to avoid problems with case-sensitivity.
- *I* - Repository ID. Reference to the repository table (see below) indicating the repository to which the user belongs.
- *E* - Repository name. The fully-qualified name by which the user is known in the repository.
- *A* - Credentials. The encrypted password and PIN.
- *B* - Lock count. The number of times the user has failed authentication since the last successful authentication.
- *F* - Reset count. The number of times the user has used self-reset since the last successful authentication.
- *D* - Message count. The index into the security strings table for the next available string.
- *J* - Encryption key (version 4.1.3 onwards). This field is used in the credential encryption.

Repositories

Table Name: PINSAFEL

Available since: 3.3 (also applies to repository ID field in Users table)

Lists the repositories from which PINsafe can import users.

NOTE: from version 3.4 to 3.8, every Agent defined in PINsafe was also listed here, since Agents are capable of creating users through the AdminXML API. From 3.9 onwards, only Agents which have the ability to act as a Repository are listed here.

Fields

- A - Repository ID - generated automatically and referenced to Users table
- B - Repository name - as shown in the admin console

Status Flags

Table Name: PINSAFES

Available since: 4.2

Lists the status of all users in the database, one record per user.

Fields:

- A - User ID
- B - PIN never expires. Set to 1 if true or 0 if false
- C - PIN must be changed after next login. Set to 1 if true or 0 if false
- D - User status. This is a single value composed of the following individual bits

Status Bits:

The corresponding bit is set to 1 if the status flag is set or 0 if not

- 1 - Deleted
- 2 - Disabled (in the repository)
- 4 - Locked by administrator / helpdesk
- 8 - Inactive
- 16 - Failed too many consecutive login attempts
- 32 - PIN expired
- 64 - Timed lockout

Policy Flags

Table Name: PINSAFEC

List of restrictions applied to each user.

Obsolete as of Sentry version 4.2, replaced by PINSAFES.

NOTE: Prior to version 3.8, each flag was created only when it was set for the first time, so it was possible for users not to have a value of a particular flag. From 3.8 onwards, all flags are created for all users (and set to 0 initially).

Fields

- C - User ID
- B - Flag type (see below)
- D - Flag value: 1 indicates set, 0 (or missing prior to 3.8) indicates not set.

Flag Types

- 0 - User disabled
- 1 - User locked
- 2 - User must change PIN after next login
- 3 - User's PIN never expires
- 4 - User is marked as deleted
- 5 - User is inactive

User Rights

Table Name: PINSAFEB

This table lists the rights a user has. Unlike the policy flags table, the presence of a record for a particular right indicates that a user has that right. The absence of such a record indicates that a user doesn't have that right.

Fields

- B - User ID
- A - Right (see below)

User Rights

- 0 - Can authenticate as single channel
- 1 - Can authenticate as dual channel
- 2 - Can authenticate using mobile client strings
- *3 - Can authenticate using RADIUS (OBSOLETE)*
- 4 - Can act as administrator
- 5 - Can act as helpdesk user
- 6 - User is PINless
- 7 - Can authenticate using telephony (version 3.9 onwards)
- 8 - Can use OATH tokens (version 3.9.6 onwards)

Security Strings

Table Name: PINSAFEF

Contains the list of current (dual channel) security strings for users.

Fields

- D - User ID
- A - String index
- B - Security String

Mobile Token Strings

Table Name: PINSAFEE

Contains the list of current mobile client security strings

Fields

- D - User ID
- A - String index
- B - Security String

Alerts Transport

Table Name: PINSAFEA

Contains the transport details for sending alerts.

Obsolete as of version 3.9.6 - replaced by User Attributes

Fields

- C - User ID
- B - Transport name (as listed in Transport -> General)
- A - Destination (e.g. email address or phone number)

Strings Transport

Table Name: PINSAFEH

Lists the transport destinations used for sending security strings.

Obsolete as of version 3.9.6 - replaced by User Attributes

Fields

- A - User ID
- B - Transport name (see alert transport)
- C - Destination (see alert transport)

Group Membership

Table Name: PINSAFEI

Lists the groups to which each user belongs

Fields

- B - User ID
- A - Group name (as listed in Repository -> Groups)

User Attributes

Table Name: PINSAFEP

Available since: 3.9.1

Auxiliary information on users, such as email address, mobile phone number, alternative usernames.

Since 3.9.6, this is the primary source of transport destinations.

Fields

- A - User ID
- B - Attribute name
- C - Attribute value

Activity

Table Name: PINSAFEN

Available since: version 3.4

Lists the time of the last activity of each type for each user.

NOTE: prior to version 3.4, this information was held in table PINSAFED, and the activity codes were different. Not all activities have been recorded in all versions of PINsafe.

Fields

- A - User ID
- C - Activity type (see below)
- D - Time of last event

Activity types

- 0 - Login
- 1 - PIN changed
- 2 - Self-reset
- 3 - User created
- 4 - Unlocked
- 5 - Locked
- 6 - PIN reset (by admin/helpdesk)
- 7 - Password reset (by admin/helpdesk)
- 8 - Disabled
- 9 - Enabled
- 10 - Marked as deleted (3.5 onwards)
- 11 - Undeleted (3.5 onwards)
- 12 - Deactivated (3.5 onwards)
- 13 - Reactivated (3.5 onwards)
- 14 - Login failed (3.6 onwards)
- 15 - Provisioned (3.7 onwards)
- 16 - Timed lockout (3.8 onwards)
- 17 - Change PIN required (3.8 onwards)

Audit

Table Name: PINSAFEM

Available since: version 3.4

This table contains a full record of all activities of the types listed by all users.

NOTE: this table only retains records for a specified time - by default 30 days, but this can be extended.

NOTE: the address field information must be supplied by the Agent, as typically there is no way for PINsafe to retrieve that information. Few Agents provide this information. For RADIUS NAS, this will be the calling station ID. Not all NAS's support this attribute, and those that do usually require configuring in order to send it.

Fields

- G - User ID
- H - User ID index (for internal use)
- I - Username
- A - Activity type (see Activity table)
- B - Address of computer from which the activity occurred (requires the information to be passed by the Agent)
- C - Detail (additional information where relevant)
- D - Name of the Repository the user belongs to
- E - Time
- F - Time index (for internal use)

Mobile Identity

Table Name: PINSAFEO

Available since: 3.8

Stores the mobile client identity and fingerprint for the user's mobile phone.

Fields

- A - Fingerprint
- B - Identity code
- C - User ID

OATH Tokens

Table Name: PINSAFEQ

Available since: 3.9.6

Stores details on the OATH tokens.

Fields

- A - Token ID (auto-generated)
- B - Token serial number
- C - User ID
- D - Token seed (encrypted)
- E - Token event count
- H - Token type ('HOTP' or 'TOTP')
- I - Date/time token imported
- J - Date/time token allocated to current user

Cached Passwords

Table Name: PINSAFER

Available since: 3.11

Stores encrypted Windows passwords for use by AuthControl Desktop.

Fields

- A - User ID
- B - Agent ID - identifies the instance of AuthControl Desktop this applies to
- C - Cached Password - this is encrypted by AuthControl Desktop and is passed back without decryption

Version

Table Name: PINSAFEK

Contains a single record indicating the current version of the database.

Fields

- A - The version number