BLUEDOT

OPERATIONS NOTE

Bootstrap and Account Recovery

Operations Note — Tokens, Passwords & Sessions

The bootstrap token issued at install time, how to recover access when the admin password is lost, and how to manage active sessions for compromised accounts — including what each recovery path writes to the audit trail.

Document Type	BlueDot Operations Note
Component	QuantumTouch — identity & bootstrap
Audience	Operators & Support Engineers
Last Updated	28 June 2026
Classification	**BlueDot Proprietary**
Date	October 2026

© 2026 BlueDot · All rights reserved.

Contents

The bootstrap token 3
"I lost the bootstrap token before creating an admin account" 3
"I created an admin but forgot the password" 3
"I forgot the admin password and there is no other admin account" 4
Force-logging out a specific user 4
Audit trail 5

What this covers: the bootstrap token issued at install time, how to recover access when the admin password is lost, and how to manage active sessions for compromised accounts.

Last updated: 2026-06-28

The bootstrap token

When the installer runs for the first time, it generates a one-time bootstrap token and prints it to the terminal:

```
[install] BOOTSTRAP TOKEN: bs_xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
```

Copy this token before closing the terminal. It is the only way to complete the first-time setup wizard and create the initial admin account. Once the first admin account is created, the token is consumed and cannot be reused.

"I lost the bootstrap token before creating an admin account"

If no admin account has been created yet, you can re-display the token:

```
sudo /opt/bng-deploy/bin/show-bootstrap-token.sh
```

This script prints the token to stdout only if the system is still in the pre-bootstrap state (no admin exists). If an admin has already been created, the script exits with an error rather than printing a stale or invalid token.

"I created an admin but forgot the password"

Reset the password for any existing user account:

```
sudo /opt/bng-deploy/bin/reset-user-password.sh <username>
```

Replace `<username>` with the account name. The script prompts you to enter a new password (confirmed twice), writes it to `users.json` using the same argon2id hash the application uses at login, and immediately invalidates all existing sessions for that user. The user (or you, on their behalf) can then log in with the new password.

This operation is logged in the audit trail as `event:auth.password_reset`.

"I forgot the admin password and there is no other admin account"

If there is no second admin account and you cannot access the UI to reset the first, use the full reset script:

```
sudo /opt/bng-deploy/bin/reset-admin.sh
```

This is destructive. The script: 1. Wipes `users.json` — all user accounts are deleted. 2. Wipes `sessions.json` — all active sessions and bearer tokens are revoked. 3. Generates a new bootstrap token. 4. Restarts the service.

After the restart, the system is in the same state as a fresh install. Go through the setup wizard again using the new bootstrap token to create a new admin account.

Use this only as a last resort. Any user accounts, API tokens, and session state that existed before the reset are permanently gone.

Force-logging out a specific user

If an account is suspected to be compromised, or if you need to invalidate all active sessions for a user without resetting their password:

1. Log in as an admin and navigate to **Users**.
2. Click the row for the target user to expand it.
3. Click **Sessions** or **Force log out** to revoke all active sessions for that user, including any bearer tokens that were minted at their last login.

The user is immediately logged out of all browser tabs and any API clients using their token. Their account and password are not changed — they can log back in with their existing credentials.

This action is logged in the audit trail as `event:auth.sessions_revoked`.

Audit trail

Every authentication event is recorded in the audit timeline. Events relevant to account management are tagged with the `event:auth.*` prefix:

Event tag	What it records
`event:auth.login`	Successful login (username, IP, session ID)
`event:auth.logout`	Explicit logout
`event:auth.login_failed`	Failed login attempt (username, IP)
`event:auth.password_reset`	Password changed via reset script or UI
`event:auth.sessions_revoked`	Force-logout of all sessions for a user
`event:auth.user_created`	New user account created
`event:auth.user_deleted`	User account deleted

To review auth events: open the audit timeline and click the **Logins** chip at the top to filter to `event:auth.*` entries only. Each entry shows the timestamp, the acting user or system process, the affected username, and the source IP where applicable.

For incident response, the raw audit log is also written to:

```
/var/lib/quantum-controller/audit.log
```

This file is append-only during normal operation and survives service restarts.