Guide Administrateur (Super-Administrateur / DSI)

Solution CA BNETD — Documentation

> Public : Super-Administrateur (profil `SUPER_ADMIN`). Accès : menu **Administration** (visible uniquement pour ce profil).

1. Connexion

1. Ouvrir l'application et saisir e-mail + mot de passe.
2. Si la double authentification (2FA) est activée sur votre compte, saisir le code à 6 chiffres.

2. Gestion des comptes utilisateurs

Administration → Utilisateurs.

Créer un compte

1. Cliquer **Nouvel utilisateur**.
2. Renseigner prénom, nom, e-mail, **profil** et un **mot de passe initial**.
3. Enregistrer. Communiquer le mot de passe initial à l'utilisateur (à changer à la première connexion).

Profils disponibles (CDC §3)

Profil	Rôle
`SUPER_ADMIN`	Administration technique, paramétrage, comptes, audit
`SECRETAIRE`	Gestion fonctionnelle : sessions, ordres du jour, convocations, PV
`PRESIDENT`	Pilotage des séances, validation des ordres du jour
`ADMINISTRATEUR`	Membre du CA : consultation, participation
`MEMBRE_COMITE`	Membre de comité spécialisé
`INVITE`	Lecture seule, ponctuelle

Modifier / suspendre / réactiver

- **Modifier** (crayon) : prénom, nom, e-mail, profil, **statut** (Actif / Suspendu / Verrouillé).
- **Suspendre** : bloque l'accès sans supprimer le compte.
- **Réactiver** : rétablit l'accès et remet à zéro le compteur d'échecs.
- **Réinitialiser le mot de passe** : depuis la fiche utilisateur (déverrouille aussi le compte).

Verrouillage automatique

Après **5 échecs** de connexion consécutifs (paramétrable), le compte passe en **Verrouillé**. Le réactiver via **Réactiver** ou en réinitialisant le mot de passe.

3. Double authentification (2FA)

Chaque utilisateur active sa propre 2FA via le menu **Sécurité & 2FA** (en haut à droite) :

1. Cliquer **Activer la 2FA** : un secret et un lien `otpauth://` s'affichent.

2. Ajouter le compte dans une application d'authentification (Google/Microsoft Authenticator, FreeOTP…) par saisie de la clé ou via le lien.
3. Saisir le code à 6 chiffres affiché pour **confirmer l'activation**.

La 2FA est ensuite exigée à chaque connexion. Elle peut être désactivée depuis le même écran.

4. Journal d'audit

Administration → Journal d'audit.

- Toutes les actions sensibles (connexions, écritures, génération de PDF, diffusion de convocations, exports…) sont **journalisées** avec **utilisateur, adresse IP et horodatage**.
- Filtrer par action (méthode HTTP, ex. `POST`).
- **Exporter (CSV)** : télécharge l'historique (ouvrable dans Excel, encodage UTF-8 avec BOM).

5. Paramétrage de la gouvernance

Le paramétrage initial (organes, comités, règles de quorum/majorité, habilitations) est chargé par `seed.sql`. Pour l'adapter à votre organisation :

- **Organes & comités** : table `organe` (type `CA` ou `COMITE`) et `comite`.
- **Règles de quorum/majorité** : table `regle_quorum` (par organe et type de session ; ex. 50 % ordinaire, 66,67 % extraordinaire).
- **Habilitations** : table `habilitation` (profil × ressource × action).

> Un écran d'administration graphique de ces paramètres est prévu dans une version ultérieure (module F). En v1, ces ajustements se font via des requêtes SQL maîtrisées par la DSI.

6. Logs applicatifs

L'application écrit ses journaux techniques dans un **fichier dédié** du répertoire `logs/` de Tomcat : **`ca-bnetd.AAAA-MM-JJ.log`** (rotation quotidienne, UTF-8), distinct de `catalina.out`.

- Contenu : démarrage de l'application, initialisation du pool de connexions, planificateur, **connexions** (réussies et échecs) et **déconnexions** avec e-mail et adresse IP, envois d'e-mails, relances/alertes automatiques, et erreurs.
- Configuration : `WEB-INF/classes/logging.properties` (handler `org.apache.juli.FileHandler` fourni par Tomcat) ; niveau `INFO` sur le package `ci.bnetd.conseil`.
- Exploitation : après un **dépôt de WAR**, laisser l'auto-déploiement se terminer (~20 s) avant d'utiliser l'application ; ne pas cliquer « Start » dans le Manager pendant ce laps.

7. Journal des e-mails

Administration → E-mails (Super-Administrateur uniquement).

- Liste des **e-mails transmis** aux membres (convocations, relances, alertes d'échéance) : date, destinataire, sujet et **statut** — *Envoyé*, *Simulé (dev)* ou *Échec*.
- **Voir** ouvre le détail avec le **corps du message** tel qu'envoyé.
- En mode démonstration (`smtp.enabled=false`), les e-mails ne sont **pas réellement expédiés** mais sont tout de même **journalisés** avec le statut *Simulé (dev)* — pratique pour vérifier le contenu sans serveur SMTP.

8. Bonnes pratiques de sécurité

- Imposer le changement des mots de passe de démonstration dès la mise en service.
- Activer la 2FA pour tous les comptes à privilèges.

- S'assurer que l'accès se fait via **HTTPS** (Nginx/TLS).
- Sauvegarder quotidiennement la base et le stockage GED.
- Consulter régulièrement le journal d'audit.
