

Resetting User Passwords in KeycloakNew Page

Password resets are a critical part of account lifecycle management. Keycloak provides multiple secure methods for resetting a user's password manually through the Admin Console, programmatically via REST API, or via user self-service workflows using email links. This guide walks through all these approaches, including configuration steps, best practices, and common issues.

Resetting Password via Admin Console

This is the most direct method for administrators to reset passwords.

Access the Admin Console

Log in to:

```
http://<your-keycloak-domain>/admin/
```

Select the desired realm.

Reset a User's Password

1. Go to **Users > [username] > Credentials**
2. Under **Set Password:**
 - Enter a new password
 - Confirm it
 - Toggle **Temporary:**
 - **ON** = user will be forced to change it on next login
 - **OFF** = permanent change
3. Click **Set Password**

The new password takes effect immediately.

Set password for root ✕

Password * 👁

New password confirmation * 👁

Temporary ? On

Resetting Password via REST API

Get Admin Access Token

```
curl -X POST "https://<keycloak-domain>/realms/master/protocol/openid-connect/token" \  
-H "Content-Type: application/x-www-form-urlencoded" \  
-d "username=admin" \  
-d "password=admin-password" \  
-d "grant_type=password" \  
-d "client_id=admin-cli"
```

Set New Password for a User

```
curl -X PUT "https://<keycloak-domain>/admin/realms/<realm>/users/<user-id>/reset-password" \  
-H "Authorization: Bearer <access_token>" \  
-H "Content-Type: application/json" \  
-d '{  
  "type": "password",  
  "value": "SecurePassword123!",  
  "temporary": false  
'
```

To get <user-id>:

```
curl -H "Authorization: Bearer <access_token>" \  
https://<keycloak-domain>/admin/realms/<realm>/users?username=<username>
```

Resetting Password via Docker CLI

Inside the Container

```
docker exec -it keycloak bash
```

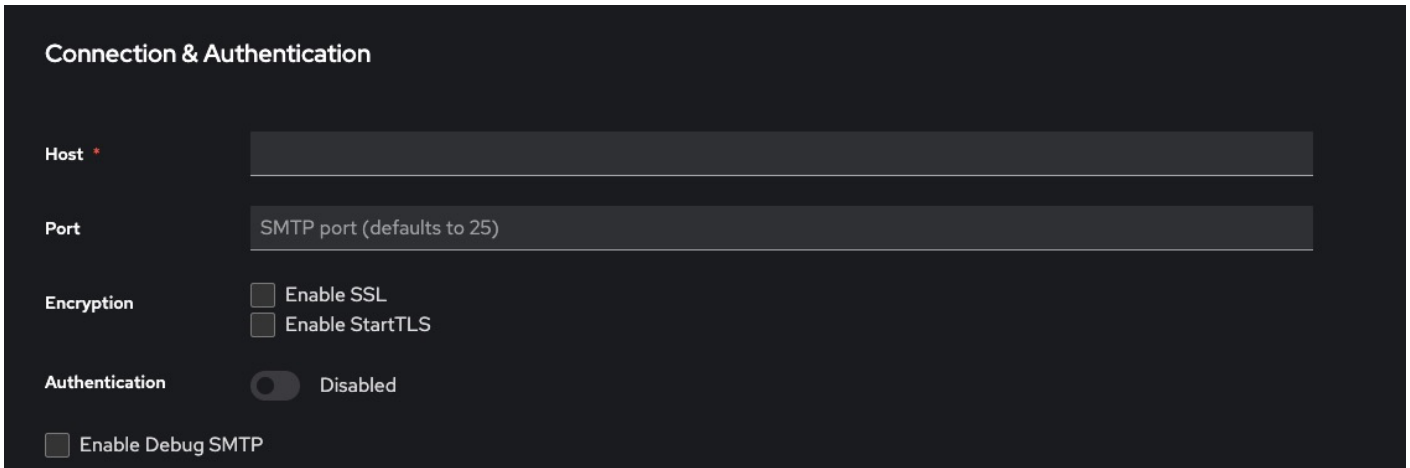
Reset User Password

```
/opt/keycloak/bin/kcadm.sh config credentials \  
--server http://localhost:8080 \  
--realm master --user admin --password admin  
  
/opt/keycloak/bin/kcadm.sh set-password -r <realm> \  
--username <username> --new-password "SecurePassword123!" --temporary=false
```

Resetting Password via Email (Self-Service)

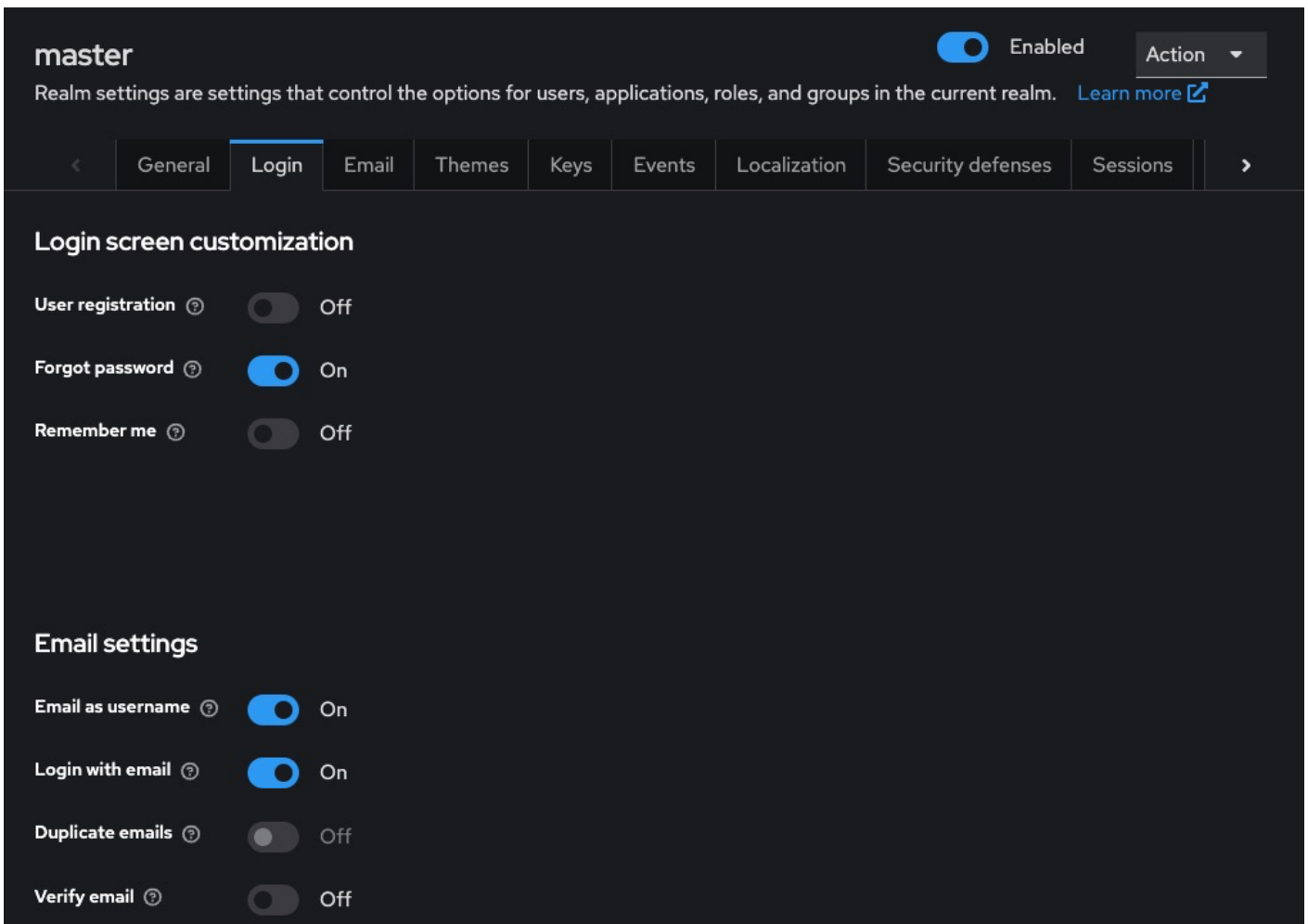
Configure SMTP

1. Go to **Realm Settings > Email**
2. Enter your SMTP configuration:
 - Host
 - Port
 - From address
 - Username/password
3. Click **Test Connection**
4. Click **Save**



Enable “Forgot Password” Option

1. Go to **Authentication > Flows > Browser**
2. Ensure **Reset Credentials** subflow is present
3. Under **Realm Settings > Login**, enable:
 - **Forgot Password**
 - **Email as Username** (optional)



Trigger Reset Link (User Side)

Users can go to the login page, click **Forgot Password**, and receive a reset link via email.

Required Permissions

- Admin Console: Must have manage-users role
- REST API: Token must have manage-users in the target realm

To assign via Admin Console:

Users > [admin-user] > Role Mappings > Realm Roles > Add 'manage-users'

Best Practices for Password Resets

- **Always Use Temporary Passwords for Manual Resets:** For admin-initiated resets, mark passwords as temporary to enforce user re-entry.
- **Secure SMTP Configuration:** Always use TLS/SSL for SMTP and avoid using free/public SMTP providers in production.
- **Limit Password Reset Frequency:** Use brute-force protection under **Realm Settings > Security Defenses > Brute Force Detection**.
- **Log and Audit Password Resets:** Enable **Events > Settings** to log password reset events and maintain an audit trail.
- **Inform Users of Security Practices:** Add disclaimers to reset emails and verify request intent using short-lived links.

Common Issues and Troubleshooting

Issue	Possible Cause	Solution
Password reset link not received	SMTP not configured or invalid	Set up SMTP under Realm Settings > Email
Reset link expired	Time limit exceeded	Increase Reset Link Lifespan under Realm Settings > Tokens
User not prompted to change password	Password not marked as temporary	Enable temporary: true or configure as required action
REST API returns 403 Forbidden	Missing permissions	Ensure admin token has manage-users role
User not found error	Wrong realm or username	Confirm realm and check Users > View all users

Revision #1

Created 2025-06-17 15:03:12 UTC by kaiwalya

Updated 2025-06-17 15:13:32 UTC by kaiwalya