

[ansible-collections](#) / [community.general](#) Public[Code](#) [Issues](#) 692 [Pull requests](#) 53 [Actions](#) [Projects](#) [Security and qu](#)[New issue](#)

# keycloak\_user module leaks credentials in verbose mode #11000

Closed#11005

Labels

bughas\_prmoduleplugins

canon-cmre-chris-conway opened on Oct 28, 2025



## Summary

Using the keycloak\_user module leaks credentials if ansible is used in verbose logging mode.

## Issue Type

Bug Report

## Component Name

keycloak\_user

## Ansible Version

```
$ ansible --version
```



```
ansible [core 2.18.10]
  config file = None
  configured module search path = ['/ansible/.ansible/plugins/modules',
'/usr/share/ansible/plugins/modules']
  ansible python module location = /usr/local/lib/python3.11/site-packages/ansible
  ansible collection location =
/ansible/.ansible/collections:/usr/share/ansible/collections
  executable location = /usr/local/bin/ansible
  python version = 3.11.11 (main, Aug 21 2025, 00:00:00) [GCC 11.5.0 20240719 (Red Hat
11.5.0-5)] (/usr/bin/python3.11)
```



```
jinja version = 3.1.6
libyaml = True
```

## Community.general Version

```
$ ansible-galaxy collection list community.general
```



```
# /usr/local/lib/python3.11/site-packages/ansible_collections
Collection      Version
-----
community.general 10.7.4
```



## Configuration

```
$ ansible-config dump --only-changed
```



## OS / Environment

RHEL 9 UBI container

## Steps to Reproduce

Call the following script: `ansible-playbook -vvv playbook.yml`

```
---
- name: Keycloak
  hosts: localhost
  tasks:
    - name: Create master realm admin user
      community.general.keycloak_user:
        auth_keycloak_url: "https://my-host:port"
        auth_realm: master
        auth_username: "temp_admin"
        auth_password: "temp_password"
        realm: master
        username: "admin-user"
        enabled: true
        credentials:
          - type: password
            value: "admin-password"
            temporary: false
```



## Expected Results

Invocation should mask password, as it does for `auth_password` :

```
"invocation": {
  "module_args": {
    "access": null,
    "attributes": null,
    "auth_client_id": "admin-cli",
    "auth_client_secret": null,
    "auth_keycloak_url": "https://staging-cosvc.eng.local:8443",
    "auth_password": "VALUE_SPECIFIED_IN_NO_LOG_PARAMETER",
    "auth_realm": "master",
    "auth_username": "temp_admin",
    "client_consents": [],
    "connection_timeout": 10,
    "credentials": [
      {
        "temporary": false,
        "type": "password",
        "value": "VALUE_SPECIFIED_IN_NO_LOG_PARAMETER"
      }
    ],
    "disableable_credential_types": [],
    "email": null,
    "email_verified": false,
    "enabled": true,
    "federated_identities": [],
    "federation_link": null,
    "first_name": null,
    "force": false,
    "groups": [],
    "http_agent": "Ansible",
    "id": null,
    "last_name": null,
    "origin": null,
    "realm": "master",
    "refresh_token": null,
    "required_actions": [],
    "self": null,
    "service_account_client_id": null,
    "state": "present",
    "token": null,
    "username": "admin-user",
    "validate_certs": true
  },
},
```



## Actual Results

Verbose output includes password. See invocation-> module\_args -> credentials -> value:

```
"invocation": {
  "module_args": {
    "access": null,
    "attributes": null,
    "auth_client_id": "admin-cli",
    "auth_client_secret": null,
    "auth_keycloak_url": "https://my_host:port",
    "auth_password": "VALUE_SPECIFIED_IN_NO_LOG_PARAMETER",
    "auth_realm": "master",
    "auth_username": "temp_admin",
    "client_consents": [],
    "connection_timeout": 10,
    "credentials": [
      {
        "temporary": false,
        "type": "password",
        "value": "admin-password"
      }
    ],
    "disableable_credential_types": [],
    "email": null,
    "email_verified": false,
    "enabled": true,
    "federated_identities": [],
    "federation_link": null,
    "first_name": null,
    "force": false,
    "groups": [],
    "http_agent": "Ansible",
    "id": null,
    "last_name": null,
    "origin": null,
    "realm": "master",
    "refresh_token": null,
    "required_actions": [],
    "self": null,
    "service_account_client_id": null,
    "state": "present",
    "token": null,
    "username": "admin-user",
    "validate_certs": true
  }
},
```



## Code of Conduct

I agree to follow the Ansible Code of Conduct



ansibullbot on Oct 28, 2025

Collaborator



Files identified in the description:

- [plugins/modules/keycloak\\_user.py](#)

If these files are incorrect, please update the `component name` section of the description or use the `!component` bot command.

[click here for bot help](#)



ansibullbot on Oct 28, 2025

Collaborator



cc [@eikef](#) [@elfelip](#) [@mattock](#) [@ndclt](#) [@thomasbach-dev](#)

[click here for bot help](#)



ansibullbot added **bug** **module** **plugins** on Oct 28, 2025



felixfontein on Oct 28, 2025

Collaborator



This also affects standard module invocation logging. You might want to check your syslog, maybe you can find the passwords in there as well... It's likely best to add `no_log: true` to the task for now.

The quick fix for this would be setting `no_log=True` for `credentials[].value`. That would *always* mask the values put in there, even if they are not passwords. I don't know whether the values are mostly passwords, or not.

Alternatively we could add passwords specified there to `module.no_log_values`. But we can only do that after `AnsibleModule` has been constructed (and validated the parameters) - which means that if parameter validation fails, the passwords are returned as in this issue. So this isn't really great.

The best solution will come eventually with data tagging in ansible-core (with a tag for sensitive data), but that won't be there before ansible-core 2.21 earliest.

I think I'm going to create a PR to add `no_log=True` to the `credentials[].value` parameter, unless someone has a better idea / reason why this isn't a good idea.



felixfontein mentioned this on Oct 28, 2025








[keycloak\\_user: mark credentials\[\].value as no\\_log=True #11005](#)




felixfontein on Oct 28, 2025

Collaborator



[#11005](#) **ansibullbot** added **has\_pr** on [Oct 28, 2025](#) **felixfontein** closed this as **completed** in [#11005](#) on [Oct 29, 2025](#) **patchback** mentioned this in 3 pull requests on [Oct 29, 2025](#) [\[PR #11005/54af64ad backport\]\[stable-9\] keycloak\\_user: mark credentials\[\].value as no\\_log=True #11010](#) [\[PR #11005/54af64ad backport\]\[stable-10\] keycloak\\_user: mark credentials\[\].value as no\\_log=True #11011](#) [\[PR #11005/54af64ad backport\]\[stable-11\] keycloak\\_user: mark credentials\[\].value as no\\_log=True #11012](#) **reanguiano** mentioned this on [Dec 5, 2025](#) [\[GHSA-8ggh-xwr9-3373\] Ansible Community General Collection is vulnerable to exposure of sensitive information github/advisory-database#6513](#) **carnil** on [Dec 6, 2025](#) · edited by **carnil**

Edits ▾ ⋮

FTR, this has [CVE-2025-14010](#) assigned. **felixfontein** on [Dec 6, 2025](#)

Collaborator ⋮

Thanks for linking to the advisory, I wasn't aware there is one. Ansible 11.x.y after 11.12.0 also contain the fix, for some reason that's not mentioned in the advisory (<https://github.com/ansible-community/ansible-build-data/blob/11.12.0/11/CHANGELOG-v11.md#security-fixes>).

[Sign up for free](#) to join this conversation on **GitHub**. Already have an account? [Sign in to comment](#)

## Metadata

### Assignees

No one assigned

### Labels

**bug** **has\_pr** **module** **plugins**

---

### Type

No type

---

### Projects

No projects

---

### Milestone

No milestone


---

### Relationships

None yet

---

### Development

 keycloak\_user: mark credentials[].value as no\_log=True  
ansible-collections/community.general

 12.0.0

---

### Participants

