

Aresh's auth demo for CMS

# Revision/update of the authentication system

- Task assigned by Julia (19 Sep 2017):
  - **E-group cric-cmstest1 via SSO (both Stephan and Giuseppe belong to cric-cmstest1)** mapped to Site Admin group able to edit CMS site model with instance-restrictions by country. The restriction should be on the country level and **country is retrieved from VOMS** (so unless the person has been logged in first time with VOMS, he/she can not edit site info, since the country is not resolved). => **Stephan can edit US sites, Giuseppe Italian sites only after VOMS login.**
  - **E-group cric-cmstest2 via SSO (only Stephan belongs to cric-cmstest2)** should be mapped to the CRIC group which is allowed to edit only T2\_IT\_Bari. => **Stephan can edit T2\_IT\_Bari via SSO login**
- **In short (see backup slides):**
  - **if Stephan logs in only via SSO, then Stephan can edit only T2\_IT\_Bari, but no other sites.**
  - **If Stephan logs in only via VOMS, then Stephan can edit all US sites, e.g. T1\_US\_FNAL, but not T2\_IT\_Bari.**
  - **If Stephan has done logins both via SSO and via VOMS, then Stephan can edit both T2\_IT\_Bari and US sites (e.g. T1\_US\_FNAL), but not other sites.**

# Revision/update of the authentication system

- ssl authentication implemented (for cric admins)
- modified implementation of 'Group' mapping for vomsauth
- modified implementation of 'Group' mapping for ssoauth
- modified cmsview ops\_edit to enable restricted permissions
- Gitlab: <https://gitlab.cern.ch/aresh/cric/commits/voms-auth>

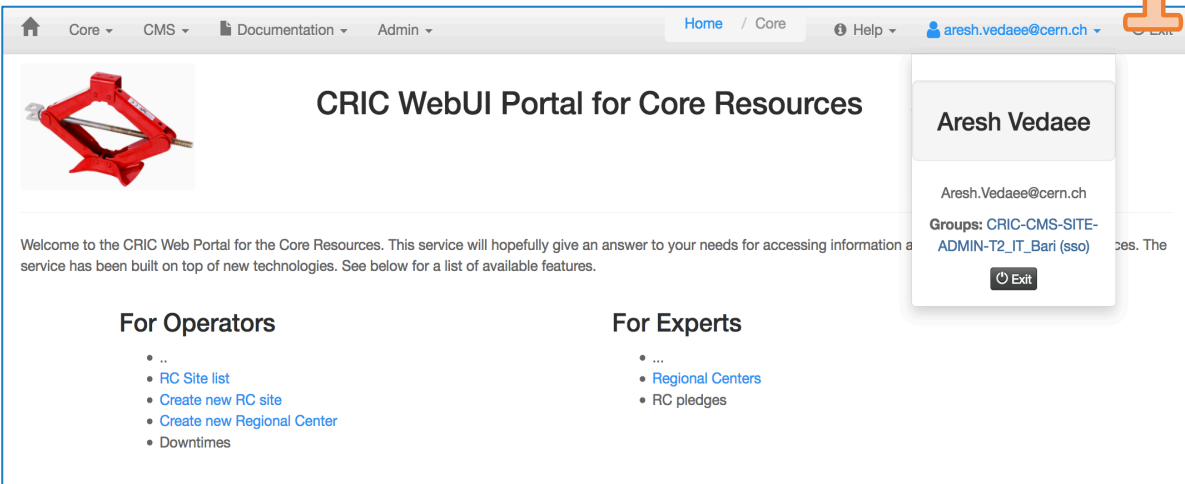
# Plan

- Complete second task assigned by Julia:
  - Map **e-group cric-cmstest3** to the CRIC group which can edit any glidein entry info without any instance restriction, but not to edit CMS site (useful for glideins factory admins).
- Implement vomsauth cron to retrieve voms users' info

**BACKUP**

# Login only via SSO

1



CRIC WebUI Portal for Core Resources

Aresh Vedaae

Aresh.Vedaae@cern.ch

Groups: CRIC-CMS-SITE-ADMIN-T2\_IT\_Bari (sso)

Exit

For Operators

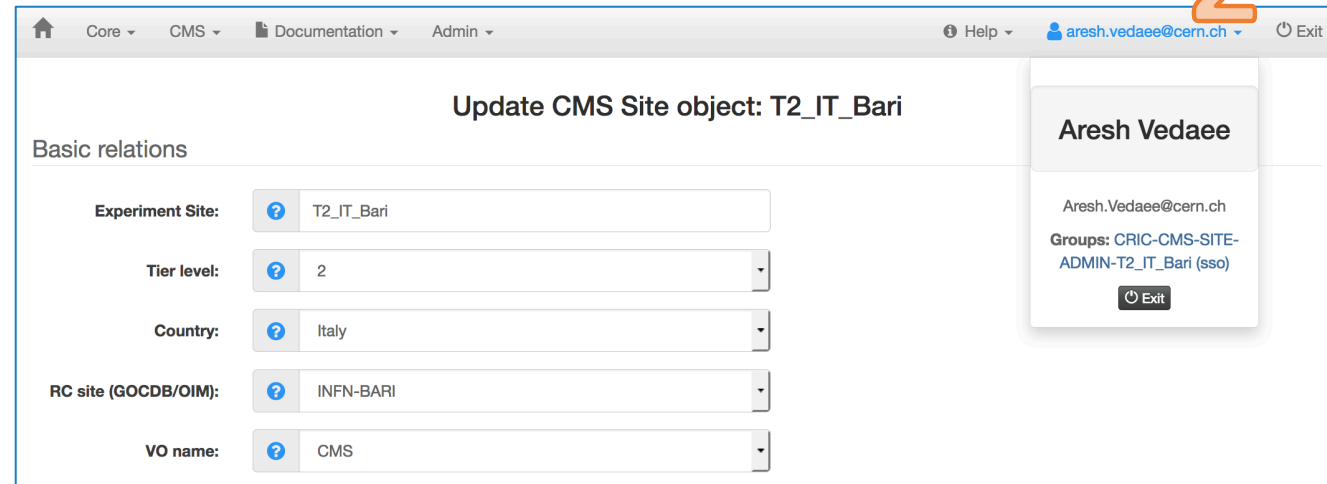
- ...
- RC Site list
- Create new RC site
- Create new Regional Center
- Downtimes

For Experts

- ...
- Regional Centers
- RC pledges

Welcome to the CRIC Web Portal for the Core Resources. This service will hopefully give an answer to your needs for accessing information and the service has been built on top of new technologies. See below for a list of available features.

2



Update CMS Site object: T2\_IT\_Bari

Aresh Vedaae

Aresh.Vedaae@cern.ch

Groups: CRIC-CMS-SITE-ADMIN-T2\_IT\_Bari (sso)

Exit

Basic relations

Experiment Site: T2\_IT\_Bari

Tier level: 2

Country: Italy

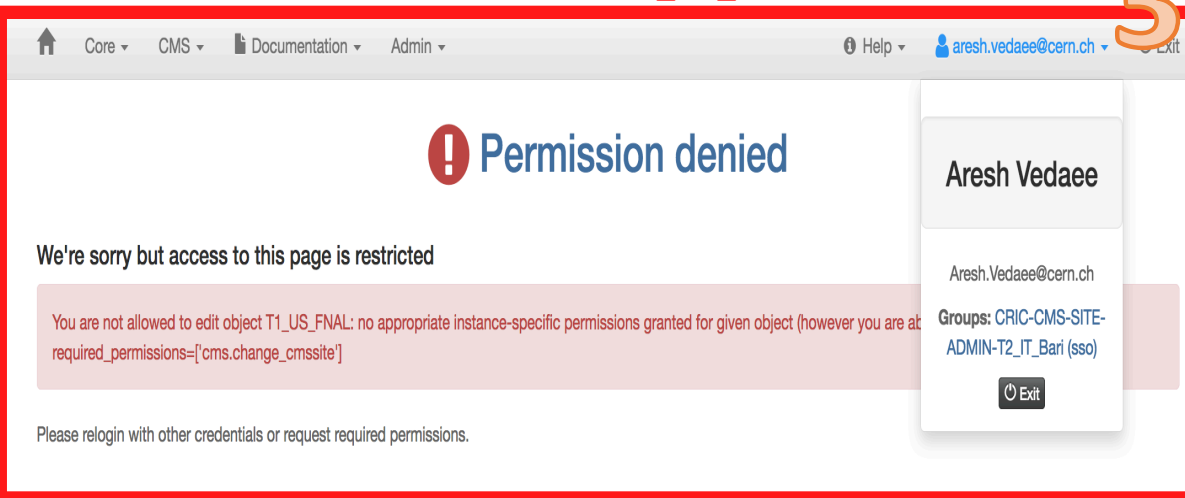
RC site (GOCDB/OIM): INFN-BARI

VO name: CMS

if I were Stephan and log in only via SSO, then I can edit only T2\_IT\_Bari, but not T1\_US\_FNAL, or any other sites.

CAN NOT EDIT T1\_US\_FNAL !!!

3



Permission denied

Aresh Vedaae

Aresh.Vedaae@cern.ch

Groups: CRIC-CMS-SITE-ADMIN-T2\_IT\_Bari (sso)

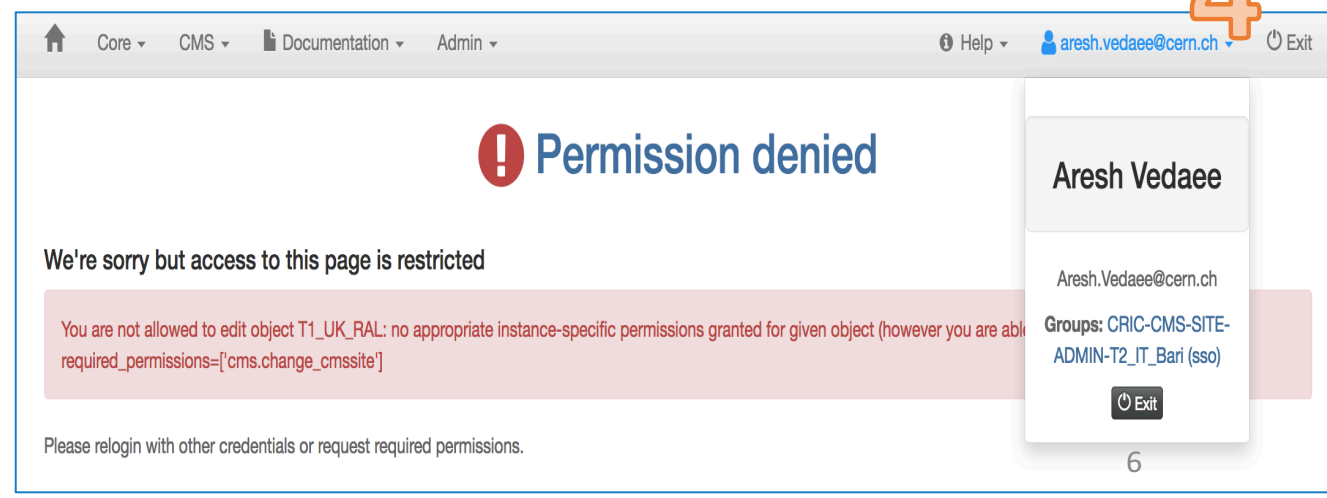
Exit

We're sorry but access to this page is restricted

You are not allowed to edit object T1\_US\_FNAL: no appropriate instance-specific permissions granted for given object (however you are able to edit objects with required\_permissions=[cms.change\_cmssite])

Please relogin with other credentials or request required permissions.

4



Permission denied

Aresh Vedaae

Aresh.Vedaae@cern.ch

Groups: CRIC-CMS-SITE-ADMIN-T2\_IT\_Bari (sso)

Exit

We're sorry but access to this page is restricted

You are not allowed to edit object T1\_UK\_RAL: no appropriate instance-specific permissions granted for given object (however you are able to edit objects with required\_permissions=[cms.change\_cmssite])

Please relogin with other credentials or request required permissions.

# Login only via VOMS

1

CRIC WebUI Portal for Core Resources

Aresh Vedaee  
Aresh.Vedaee@cern.ch  
Groups: CRIC-CMS-REGIONAL-ADMIN-US (voms)  
Exit

For Operators

- ...
- RC Site list
- Create new RC site
- Create new Regional Center
- Downtimes

For Experts

- ...
- Regional Centers
- RC pledges

if I were Stephan and log in only via VOMS, then I can edit only T1\_US\_FNAL, but not T2\_IT\_Bari, or any other non-US sites.

2

CAN NOT EDIT T2\_IT\_BARI !!!

Permission denied

We're sorry but access to this page is restricted

You are not allowed to edit object T2\_IT\_Bari: no appropriate instance-specific permissions granted for given object (however you are able to edit object T1\_US\_FNAL) (required\_permissions=["cms.change\_cmssite"])

Please relogin with other credentials or request required permissions.

3

Update CMS Site object: T1\_US\_FNAL

Aresh Vedaee  
Aresh.Vedaee@cern.ch  
Groups: CRIC-CMS-REGIONAL-ADMIN-US (voms)  
Exit

Basic relations

Experiment Site: T1\_US\_FNAL

Tier level: 1

Country: USA

RC site (GOCDB/OIM): USCMS-FNAL-WC1

VO name: CMS

4

Permission denied

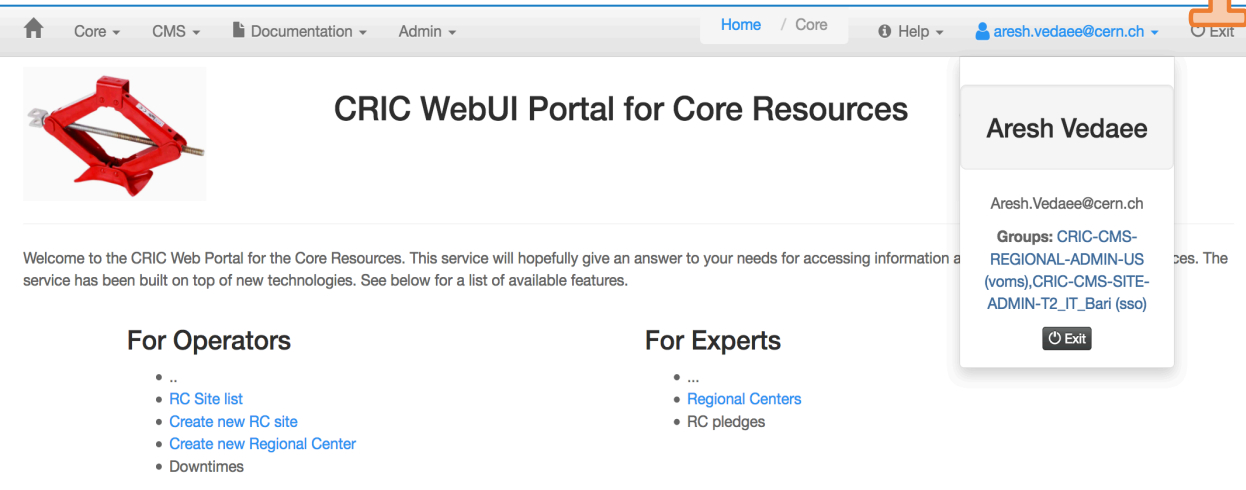
We're sorry but access to this page is restricted

You are not allowed to edit object T1\_UK\_RAL: no appropriate instance-specific permissions granted for given object (however you are able to edit object T1\_US\_FNAL) (required\_permissions=["cms.change\_cmssite"])

Please relogin with other credentials or request required permissions.

# Logins via VOMS/SSO <sup>1</sup>

If I were Stephan and have done VOMS/SSO logins, then I can edit both T2\_IT\_Bari and T1\_US\_FNAL but no other sites



CRIC WebUI Portal for Core Resources

Welcome to the CRIC Web Portal for the Core Resources. This service will hopefully give an answer to your needs for accessing information and services. The service has been built on top of new technologies. See below for a list of available features.

**For Operators**

- ..
- RC Site list
- Create new RC site
- Create new Regional Center
- Downtimes

**For Experts**

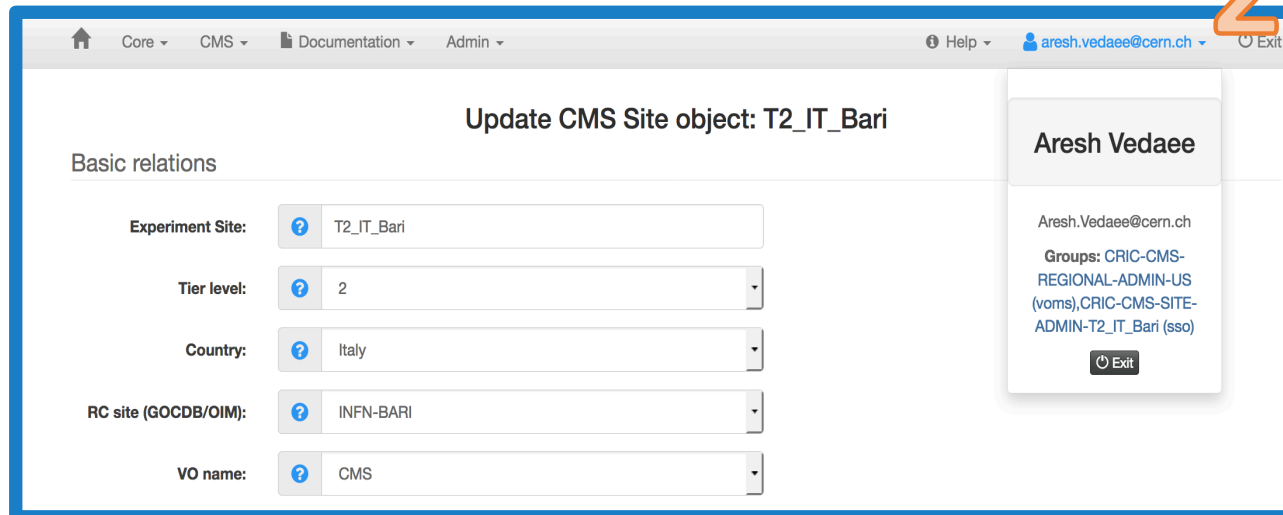
- ..
- Regional Centers
- RC pledges

**Aresh Vedaae**

Aresh.Vedaae@cern.ch

Groups: CRIC-CMS-REGIONAL-ADMIN-US (voms), CRIC-CMS-SITE-ADMIN-T2\_IT\_Bari (sso)

Exit



Update CMS Site object: T2\_IT\_Bari

Basic relations

Experiment Site: T2\_IT\_Bari

Tier level: 2

Country: Italy

RC site (GOCDB/OIM): INFN-BARI

VO name: CMS

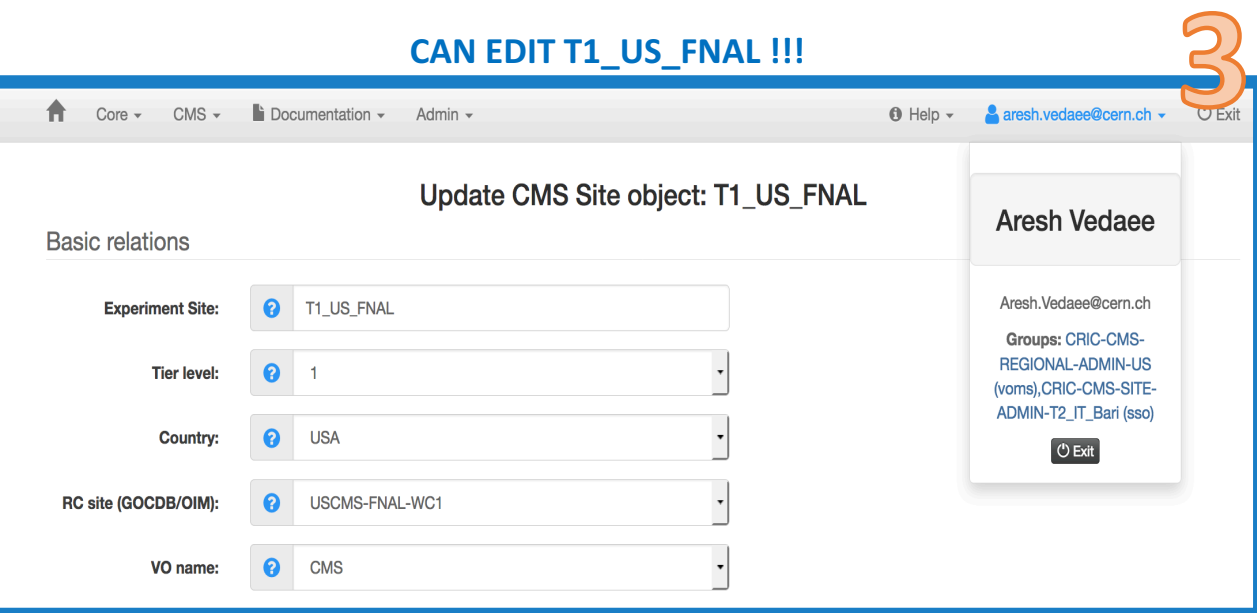
**Aresh Vedaae**

Aresh.Vedaae@cern.ch

Groups: CRIC-CMS-REGIONAL-ADMIN-US (voms), CRIC-CMS-SITE-ADMIN-T2\_IT\_Bari (sso)

Exit

**CAN EDIT T2\_IT\_Bari !!!** <sup>2</sup>



Update CMS Site object: T1\_US\_FNAL

Basic relations

Experiment Site: T1\_US\_FNAL

Tier level: 1

Country: USA

RC site (GOCDB/OIM): USCMS-FNAL-WC1

VO name: CMS

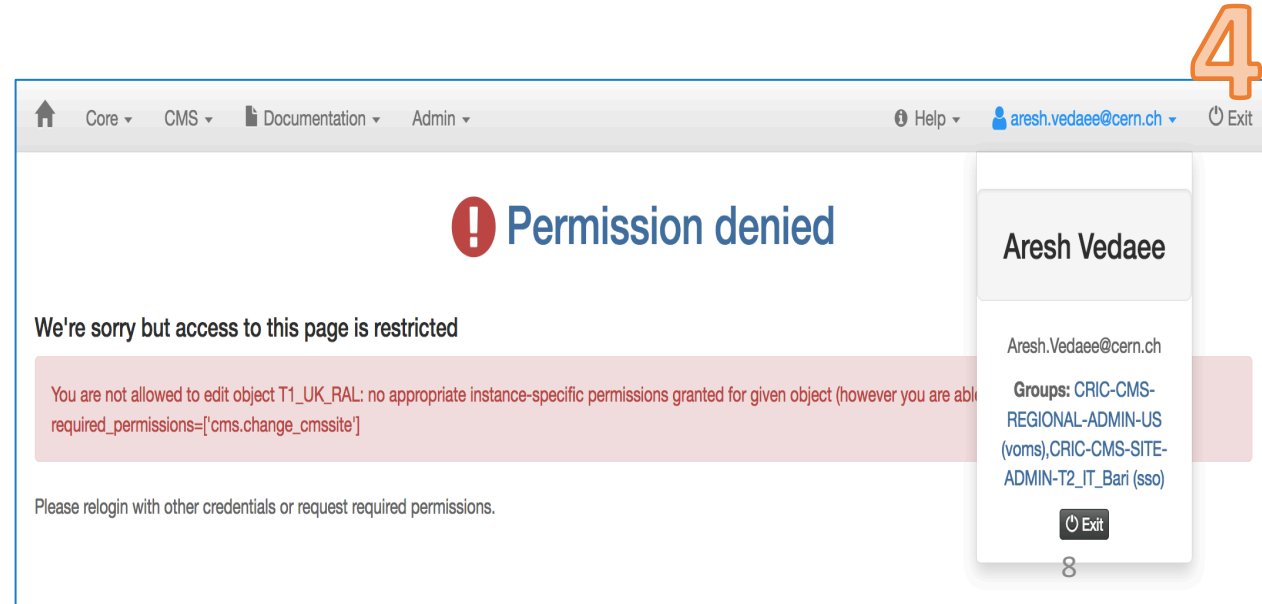
**Aresh Vedaae**

Aresh.Vedaae@cern.ch

Groups: CRIC-CMS-REGIONAL-ADMIN-US (voms), CRIC-CMS-SITE-ADMIN-T2\_IT\_Bari (sso)

Exit

**CAN EDIT T1\_US\_FNAL !!!** <sup>3</sup>



**! Permission denied**

We're sorry but access to this page is restricted

You are not allowed to edit object T1\_US\_FNAL: no appropriate instance-specific permissions granted for given object (however you are able to edit other objects) (required\_permissions=[cms.change\_cmssite])

Please relogin with other credentials or request required permissions.

**Aresh Vedaae**

Aresh.Vedaae@cern.ch

Groups: CRIC-CMS-REGIONAL-ADMIN-US (voms), CRIC-CMS-SITE-ADMIN-T2\_IT\_Bari (sso)

Exit

**4**