

# 5.6 Ensure access to the su command is restricted (Scored)

## Profile Applicability

```
Level 1 - Server  
Level 1 - Workstation
```

## Description

The su command allows a user to run a command or shell as another user. The program has been superseded by sudo, which allows for more granular control over privileged access. Normally, the su command can be executed by any user. By uncommenting the pam\_wheel.so statement in /etc/pam.d/su, the su command will only allow users in the wheel group to execute su.

## Rationale

Restricting the use of su, and using sudo in its place, provides system administrators better control of the escalation of user privileges to execute privileged commands. The sudo utility also provides a better logging and audit mechanism, as it can log each command executed via sudo, whereas su can only record that a user executed the su program.

## Audit

Run the following command and verify output includes matching line:

```
# grep pam_wheel.so /etc/pam.d/su  
auth required pam_wheel.so use_uid
```

Run the following command and verify users in wheel group match site policy:

```
# grep wheel /etc/group  
wheel:x:10:root,<user list>
```

## Remediation

Add the following line to the /etc/pam.d/su file:

```
auth required pam_wheel.so use_uid
```

Create a comma separated list of users in the wheel statement in the /etc/group file:

```
wheel:x:10:root,<user list>
```

From:

<https://secscan.acron.pl/> - **SecScan**

Permanent link:

<https://secscan.acron.pl/ubuntu1604/5/6>

Last update: **2017/05/04 12:24**

