# SCAP tailored controls from DISA STIG for RHEL6

## References

* <https://github.com/OpenSCAP/openscap>
* <https://github.com/ComplianceAsCode/content>

### HIGH impact tailored controls

#### Enable FIPS Mode in GRUB2

* Rule ID: *xccdf\_org.ssgproject.content\_rule\_grub2\_enable\_fips\_mode*
* Full FIPS mode is not available in the AWS us-east cloud as the hardware is not guaranteed to be certified. However, this site makes use of FIPS compliant openssl software and SSL certificates.

#### Install Virus Scanning Software

* Rule ID: *xccdf\_org.ssgproject.content\_rule\_install\_antivirus*
* This site employs ClamAV for anti-virus scanning and updates the database daily.

#### Ensure Software Patches Installed

* Rule ID: *xccdf\_org.ssgproject.content\_rule\_security\_patches\_up\_to\_date*
* Software patches are installed twice monthly.

### MEDIUM impact tailored controls

#### Install Smart Card Packages For Multifactor Authentication

* Rule ID: *xccdf\_org.ssgproject.content\_rule\_install\_smartcard\_packages*
* Console and smart card logins are disallowed.

#### Enable Smart Card Login

* Rule ID: *xccdf\_org.ssgproject.content\_rule\_smartcard\_auth*
* Console and smart card logins are disallowed.

#### Set Lockout Time for Failed Password Attempts

* Rule ID: *xccdf\_org.ssgproject.content\_rule\_accounts\_passwords\_pam\_faillock\_unlock\_time-storage\_disabled*
* Passwords are only used after SSH key login by administrators to achieve root access. Only administrators have accounts; two-factor authentication is used and the accounts are audited monthly.

#### Set Password Maximum Consecutive Repeating Characters

* Rule ID: *xccdf\_org.ssgproject.content\_rule\_accounts\_password\_pam\_maxrepeat*
* Passwords are only used after SSH key login by administrators to achieve root access. Only administrators have accounts; two-factor authentication is used and the accounts are audited monthly.