

## Topic: Security - Enabling C<sup>2</sup>

### *VXServices, LLC*

1230 Hunter Court, Longmont, CO 80501

Voice 303-651-6519 Fax 303-651-7693

# Solution Report

### Symptoms/Condition:

Need to enable high (C<sup>2</sup>) security in SCO Unix.

### Solution:

Before performing this operation, it is recommended that you perform a complete backup of the controller. See the "Backup/Restore Procedures Manual" for instruction.

To enable C<sup>2</sup> security:

1. Reboot the controller. At the boot prompt, press "enter". When it prompts you to proceed with normal startup or enter system maintenance mode, type the root password to enter system maintenance (single user) mode.
2. Type **sysadmsh** to enter the system administration shell.
3. Select **system**, then **configure**, then **security**. Press **F3** to list options, then select **high** security. When the system reboots, C<sup>2</sup> security will be enabled.
4. To quit sysadms, press **esc** until you return to the main menu, then select **quit**.

Use the sysadmsh to view account information and to audit accounts. Also, if existing accounts are rendered invalid by enabling C<sup>2</sup> you can change the account password expiration periods by selecting **account** in the sysadmsh and changing the values you wish. Expiration times can be set to "infinite" to enable you to go in and update the passwords in the user's account. To change a user's password, simply type **passwd** while logged into into the user's account, then follow the commands given.