

## Self-Managed Machine Checklist

The goal of this document is to educate prospective users of the trade-offs involved in having a self-managed machine (be it Windows, or Linux). CSG has an SLA (service level agreement) located at [http://www.divms.uiowa.edu/csg/policy/CSG\\_Linux\\_Support\\_Policy\\_v1.1.pdf](http://www.divms.uiowa.edu/csg/policy/CSG_Linux_Support_Policy_v1.1.pdf) and [http://www.divms.uiowa.edu/csg/policy/windows\\_sla.pdf](http://www.divms.uiowa.edu/csg/policy/windows_sla.pdf) that fully documents support responsibilities. Please review those documents and the [http://www.divms.uiowa.edu/csg/policy/CSG\\_Acceptable\\_Use\\_Policy\\_v1.4.pdf](http://www.divms.uiowa.edu/csg/policy/CSG_Acceptable_Use_Policy_v1.4.pdf) before proceeding.

Basically, there are three tiers of support offered by the CSG:

1. **CSG managed.** CSG has exclusive root/administrator privileges. CSG is responsible for software updates, patching and maintenance.
2. **Self administered with CSG load.** CSG to provide image-based initial load. Primary user must install and maintain all software (CSG may be requested to perform OS patching).
3. **Self administered.** User does load, installs and maintains software and patches.

### What responsibility am I taking by choosing to self manage my machine?

1. Administration. **You are the administrator.** Research and maintain OS patches (weekly at a minimum) to ensure the workstation is patched (or have CSG do this as defined in the appropriate Managed Machine SLA).
2. User must comply with the <http://cio.uiowa.edu/policy/policy-backup-recovery.shtml>. The easiest way to comply with this is to store all of your work on the CSG file server. Otherwise, you will have to read and comply with the policy and its off site storage requirements and tape retention policies.
3. Backup any applications, data or configuration data. **CSG does not perform client backups.**
4. Diagnose hardware compatibility issues and recover from hardware failures including data recovery.
5. Ensure system does not become compromised and reload the machine should it become compromised including coordination with ITS on port re-enablement. This involves regularly reviewing your systems log files (syslog or windows event log). Remember, there is no firewall at the University. All systems and their TCP/IP ports are accessible from the Internet .
6. Acquire, install, configure, and maintain all software applications and the OS. CSG can loan out CD's for the software that we maintain on the managed machines. Licensing and configuration will be the user's responsibility. CSG can install the managed Windows or Linux load with all of the applications in the managed load by request.
7. Ensure any licensed software has been approved by the UI legal team. The legal team has become more proactive in ensuring compliance with licensing agreements due to

export control legislation passed recently. All license agreements must be reviewed and approved by legal. Tracey Schmidt ([tracey-schmidt@uiowa.edu](mailto:tracey-schmidt@uiowa.edu)) has been coordinating communication with the appropriate people in legal.

8. Configure the firewall and harden the system shutting off all unnecessary services, restricting access via IP. See [Appendix 1](#) for details. Do this before you connect to the network otherwise there is a good chance your machine will be infected before you even finish the load if it is Windows!
9. Configure networking including name resolution (DNS), default route. See [Appendix 1](#) for details.
10. Samba mount the file shares to access your home directory. See [Appendix 1](#) for details.
11. Optionally configure your mail client.
12. Create/maintain print queues. See [Appendix 1](#) for details.
13. User account administration. Create and maintain user accounts for the system.

## Appendix 1

### 1. How do I set-up a Samba mount point to my home directory? For windows please see the doc's at

<http://www.divms.uiowa.edu/help/windows/networkdrive/>

As root run the following command:

```
mount -t smbfs -o username=username //pcnfs/username /home/username
```

### 2. How do I set-up print queues? CSG uses CUPS. Most Linux systems have a CUPS client installed by default. Enable the startup of cups and the CSG print queues should automatically show up as we have "browsing" enabled. For windows please see the doc's at

<http://www.divms.uiowa.edu/help/windows/printers/>

### 3. What is the DNS, networking, and routing information needed to configure my system?

```
# cat /etc/resolv.conf
domain divms.uiowa.edu
search divms.uiowa.edu cs.uiowa.edu math.uiowa.edu stat.uiowa.edu
uiowa.edu
nameserver 128.255.44.139
nameserver 128.255.132.9
nameserver 128.255.1.3
```

The default router for MLH is 128.255.44.1 and for SH is 128.255.132.1. The subnetmask for MLH is 255.255.254.0 and for SH is 255.255.255.0 .

### 4. What do you mean by "harden my system"? For a general overview on security for Linux and Windows, visit the <http://cio.uiowa.edu/ITsecurity/> that detail minimum security steps. For Linux, this as a minimum would involve creating a root password that is long and hard to remember, disabling all inetd services not required and setting up your /etc/hosts.allow and /etc/hosts.deny. Here is an example of the /etc/hosts.deny and /etc/hosts.allow:

```
# cat /etc/hosts.allow
#
# hosts.allow This file describes the names of the hosts which are
# allowed to use the local INET services, as decided
# by the '/usr/sbin/tcpd' server.
#
sendmail: 127.0.0.1
```

```
sshd: .uiowa.edu
```

```
# cat /etc/hosts.deny
```

```
#
```

```
# hosts.deny This file describes the names of the hosts which are
```

```
# *not* allowed to use the local INET services, as
```

```
decided
```

```
#
```

```
by the '/usr/sbin/tcpd' server.
```

```
#
```

```
ALL: ALL
```