

Network Controller / License Manager Operations Guide

For Centurion Guard®, DriveShield®, and MacShield® software Rev. 1.2.3



CONTENTS

System Requirements	1
Install/Uninstall	2
Overview	3
Enabling Selected Clients	5
Disabling Selected Clients	6
Enabling Individual Clients	6
Disabling Individual Clients	7
Changing Passwords	8
Setting Password (Centurion Guard)	9
License Manager (DriveShield)	10
Command Line Usage	12

Network Controller / License Manager - System Requirements

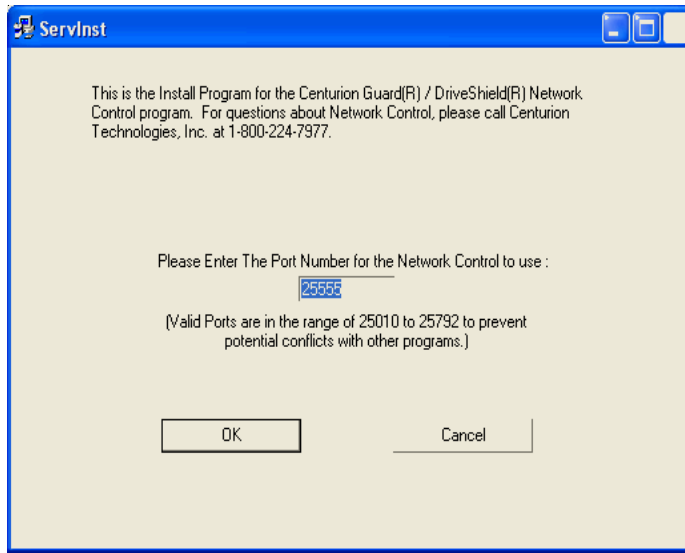
1

Network Controller / License Manager - Minimum Requirements (Server)

- PC running Windows 9x/NT/Me/2000/XP
- Recommended hardware requirements for the installed OS
- TCP/IP must be installed
- Microsoft Internet Explorer 4.01 or better

Installation

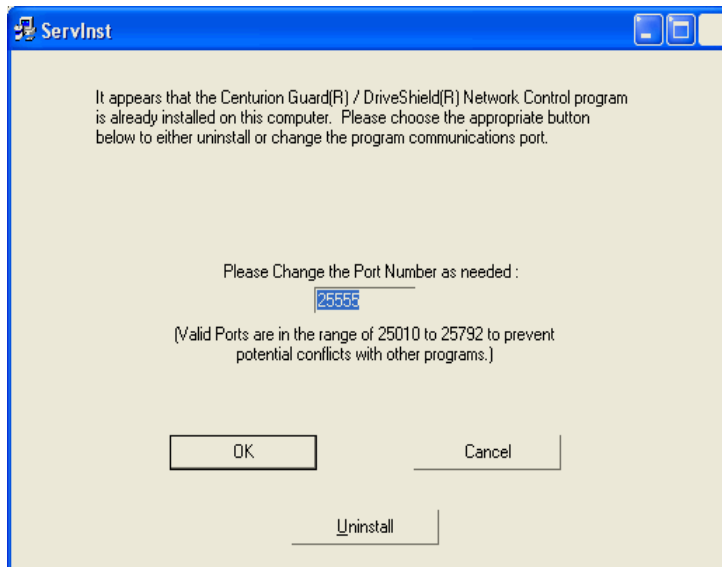
1. Browse to the location of the installation package. (i.e. D:\ or E:\ if you are installing from a CD-ROM)
2. Double-click NCLMInst.exe on your installation disk.
3. Enter the Port Number that Network Controller / License Manager will use to connect with the clients. The default is 25555. (Valid ports are in the range of 25010 to 25792) (Fig. 1.0.0)
4. Click **OK** to complete the installation. (Fig. 1.0.0)



(Fig. 1.0.0)

Removal

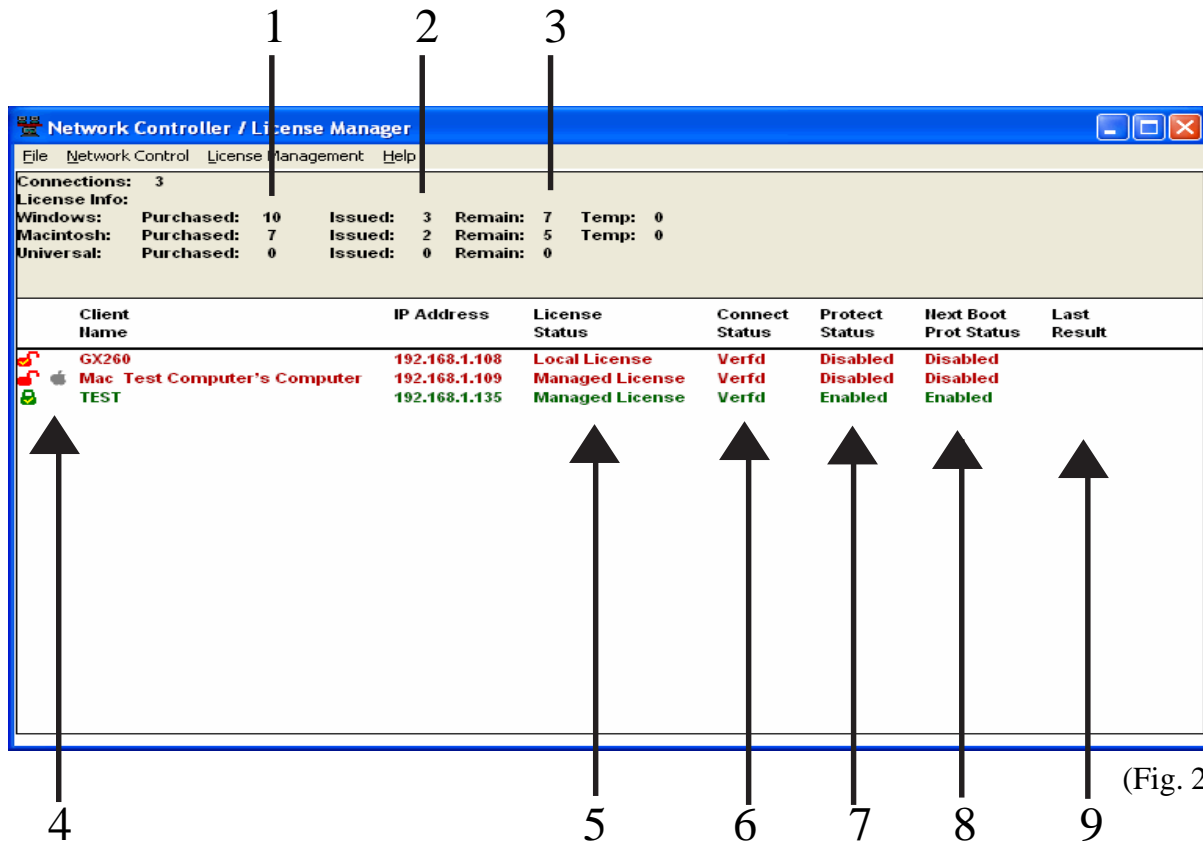
1. Browse to the location of the installation package. (i.e. D:\ or E:\ if you are installing from a CD-ROM)
2. Double-click ServInst.exe on your installation disk.
3. Click **Uninstall** to remove Network Controller / License Manager Server from the system. (Fig. 1.1.0)



(Fig. 1.1.0)

Below is a description of each field and column located on the NCLM user interface. The interface is split into two sections. The top section indicates statistics. The bottom portion of the interface will contain a list of clients that are connected to NCLM. (Fig. 2.0.0)

Note: The top section shows the three different types of licenses available. The Universal license is compatible on both Macintosh and Windows systems.



(Fig. 2.0.0)

1. **Purchased** - The number of licenses purchased and added to this server. (Software Only)
2. **Issued** - The number of licenses issued to the workstations. (Software Only)
3. **Remain** - The number of licenses available for issuance. (Software Only)
4. **Macintosh** - The apple signifies that the client is a Macintosh machine.
5. **License Status** -
 - Managed licensed* - DriveShield or MacShield software has already been licensed by the License Manager.
 - Local license* - DriveShield or MacShield is registered locally.
 - Hardware* - Centurion Guard is installed.
 - Issued* - DriveShield or MacShield requested and was issued a license.
 - ReIssued* - DriveShield or MacShield has been issued a license for that workstation but has requested it again.
 - Temp* - License Manager has issued a temporary license to a workstation.
 - Denied* - DriveShield or MacShield is requesting a license but the License Manager does not have any available to issue.
 - Trial* - DriveShield or MacShield is in the trial period and is not requesting a license.
 - Stand By* - Please wait. Verification is in process.
 - Invalid* - License is invalid. Invalid local license and Denied by License Manager.
 - No Request* - The client is not requesting a license.
 - No Err* - No error has occurred.

Continued on next page.

6. **Connect Status** - Connection status between the client and the server.

Vpend - Verification pending. Attempting verification.

Verfd - The connection has been verified.

Ukn - Connection Status is unknown.

7. **Protect Status** - Current protection status.

Enabled - Currently protected.

Disabled - NOT currently protected.

Disabled w/Key - Centurion Guard is disabled with the key.

Unknown - Unable to get protection status.

8. **Next Boot Prot Status** - Protection status for the next reboot.

Protect - Currently protected.

NotProt - NOT currently protected.

Disabled w/Key - Centurion Guard is disabled with the key.

Unknown - Unable to get protection status.

9. **Last Result** - Result of the last action..

No More Tries - The maximum number of incorrect attempts to enter that password has been reached.

Invalid Password - An incorrect password was entered.

Password too Short - Password must be at least 6 characters in length.

Password Changed - The password has been successfully changed.

Password Set - The password has been successfully set.

Enabled - The protection has been enabled.

Disabled - The protection has been disabled.

Set DS password not allowed - The password cannot be set on DriveShield protected systems.

Disabled w/Key - The Centurion Guard protection has been disabled with the key.

Error: Disable w/Key - Cannot complete action because the key is in the enabled position.

Licensed Released - The license has been successfully released.

Unable To Release - Unable to release the license.

Protected, Can't release - Cannot release the license in protected (enabled) mode.

Unknown License - Cannot obtain license information for that system.

Unknown result - Unknown error. Contact Technical Support.

The color of each client listed in the client list will help to quickly determine the Protection and Next Boot Protection Statuses. The table below explains the meaning of each color. (Fig. 3.0.0) To utilize certain features of the Network Controller on Centurion Guard protected systems, it is necessary for the key to be in a certain position (enabled or disabled). Please refer to the table below to determine what position the key should be. (Fig. 3.0.1)

Protection Status	Next Boot Protection Status	Color
Not Protected	Not Protected	Red
Not Protected	Protected	Light Green
Protected	Not Protected	Light Red
Protected	Protected	Green

(Fig. 3.0.0)

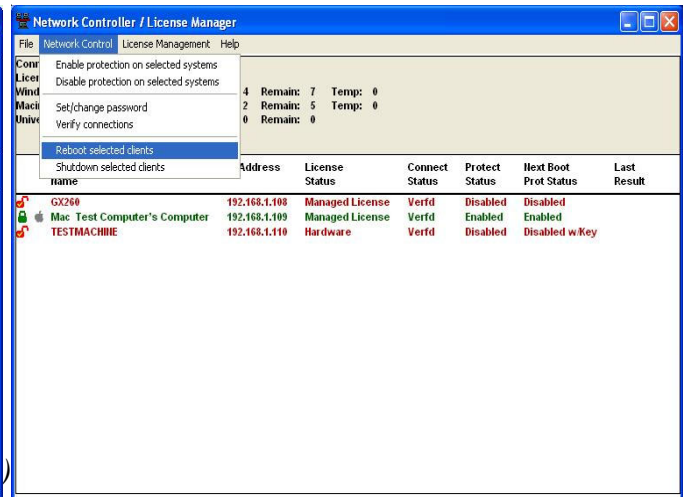
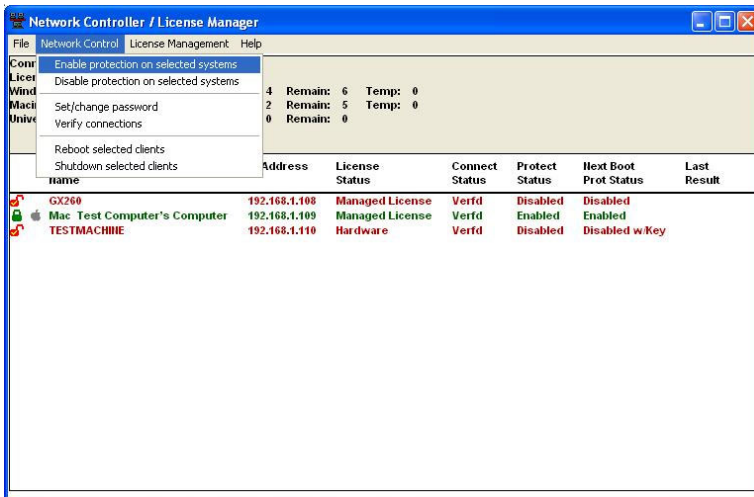
Key Position	Network Controller	Protection Status
Disabled	Disabled	Disabled
Disabled	Enabled	Disabled
Enabled	Disabled	Disabled
Enabled	Enabled	Enabled

(Fig. 3.0.1)

Controlling Selected Clients - Enabling Selected Clients

1. Click on Clients of Interest. To highlight multiple clients hold the “Shift” key while selecting clients.
2. Select **Enable Protection on Selected Systems** from the **Network Controller** drop-down menu. (Fig. 3.1.0)
3. The status displayed in the *Next Boot Status* column will change and indicate the protection AFTER reboot.
4. Select **Reboot Selected Clients** from the **Network Controller** drop-down menu to reboot ALL systems. (Fig 3.1.1)
5. A dialog box will appear with the option to **Reboot Now** or **Delayed Reboot**. (Fig 3.1.2)

Note: **Delayed Reboot** will warn the user to save their work as the system will reboot in approximately 120 seconds (2 minutes).

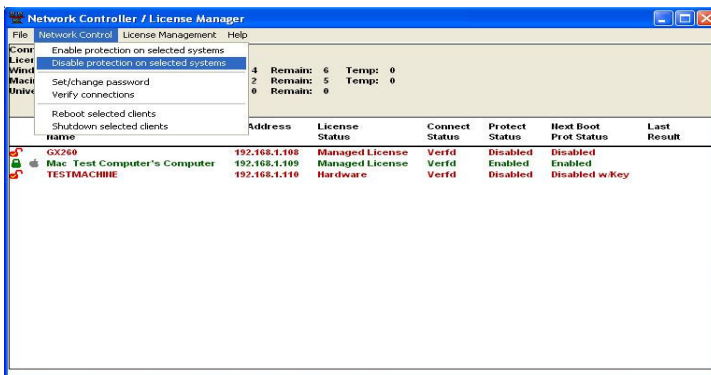


Note: To enable the Centurion Guard the key has to be in the enabled position. The Centurion Guard cannot be enabled with the key in the disabled position.

Controlling Selected Clients - Disabling Selected Clients

1. Click on Clients of Interest. To highlight multiple clients hold the “Shift” key while selecting clients.
2. Select **Disable Protection on Selected Systems** from the **Network Controller** drop-down menu. (Fig. 3.2.0)
3. Enter the password to disable DriveShield software. (Fig 3.2.1)
4. The status displayed in the *Next Boot Status* column will change and indicate the protection AFTER reboot.
5. Select **Reboot Selected Clients** from the **Network Controller** drop-down menu to reboot ALL systems. (Fig. 3.2.3)
6. A dialog box will appear with the option to **Reboot Now** or **Delayed Reboot**. (Fig 3.2.2)

Note: **Delayed Reboot** will warn the user to save their work as the system will reboot in approximately 120 seconds (2 minutes).



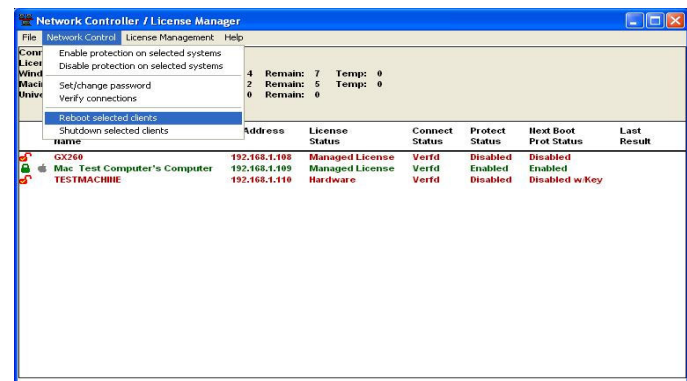
(Fig. 3.2.0)



(Fig. 3.2.1)



(Fig. 3.2.2)

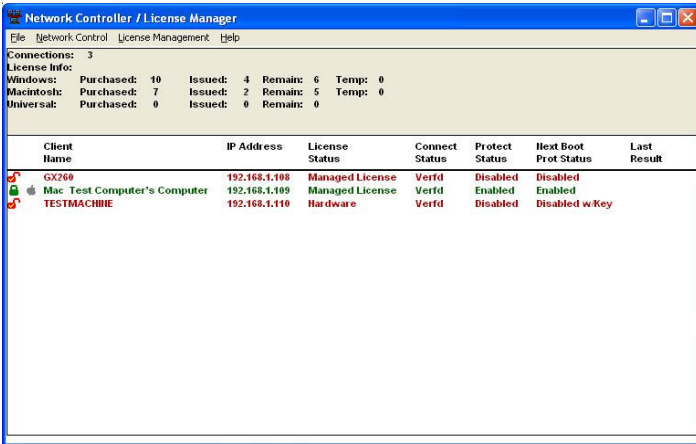


(Fig. 3.2.3)

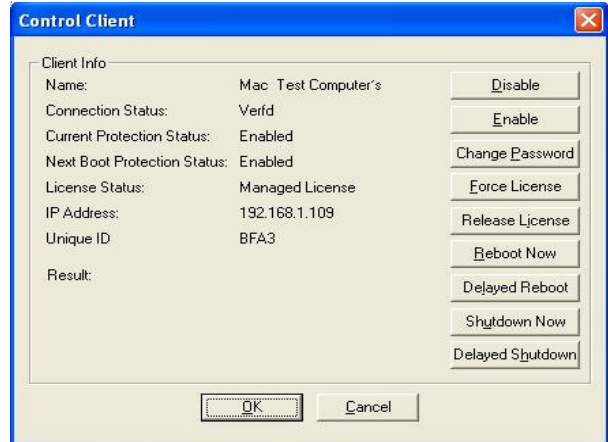
Controlling Individual Clients - Enabling

1. Double-click on the client of interest. (Fig 3.3.0)
2. A dialog box will appear like the one below with several options. Select **Enable** to enable the protection for the next boot. (Fig 3.3.1)
3. The status displayed in the *Next Boot Status* column will change and indicate the protection AFTER reboot.
4. Now, select either **Reboot Now** or **Delayed Reboot** to reboot the system for the changes to take effect. (Fig 3.3.1)

Note: **Delayed Reboot** will warn the user to save their work as the system will reboot in approximately 120 seconds (2 minutes).



(Fig. 3.3.0)

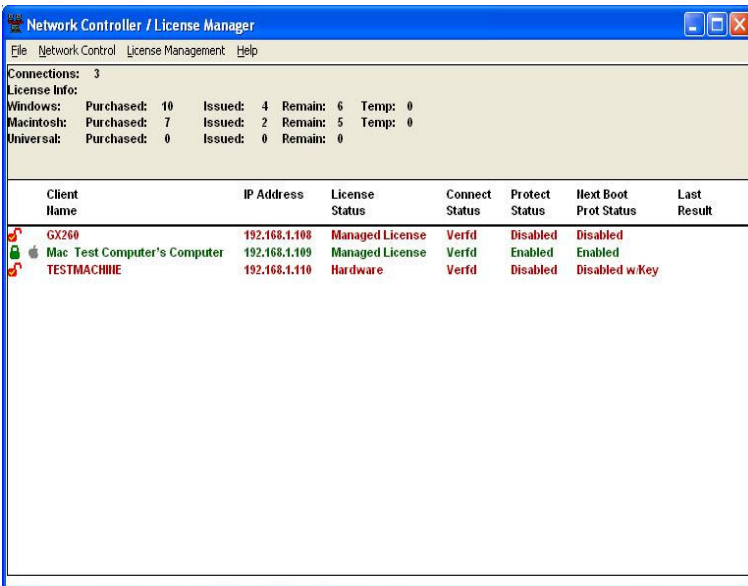


(Fig. 3.3.1)

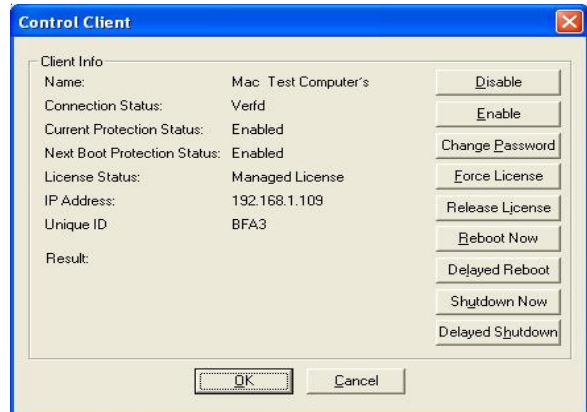
Controlling Individual Clients - Disabling

1. Double-click on the client of interest. (Fig 3.4.0)
2. A dialog box will appear with the option to **Enable**, **Disable**, **Reboot Now** and **Delayed Reboot**. Select **Disable** to disable the protection for the next boot. (Fig 3.4.1)
3. A dialog box will appear to enter the password that will disable DriveShield software. Enter the password and select **OK**. (Fig 3.4.2)
4. The status displayed in the *Next Boot Prot Status* column will change and indicate the protection AFTER reboot.
5. Now, select either **Reboot Now** or **Delayed Reboot** to reboot the system for the changes to take effect. (Fig 3.4.1)

Note: **Delayed Reboot** will warn the user to save their work as the system will reboot in approximately 120 seconds (2 minutes).



(Fig. 3.4.0)



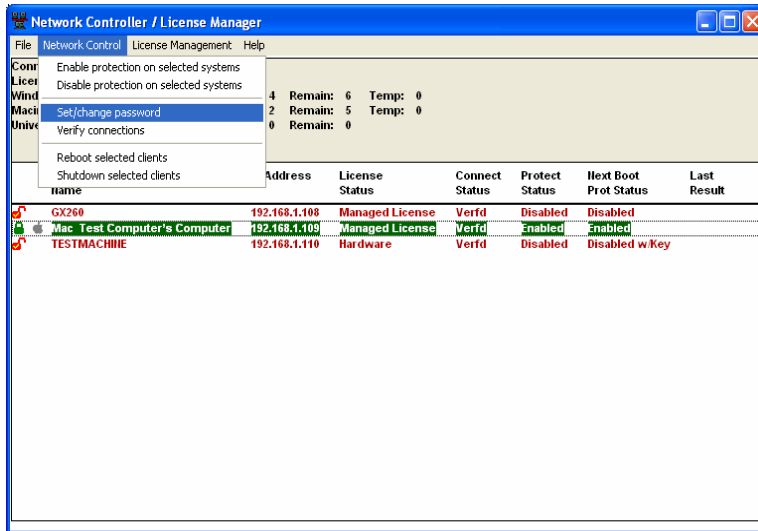
(Fig. 3.4.1)



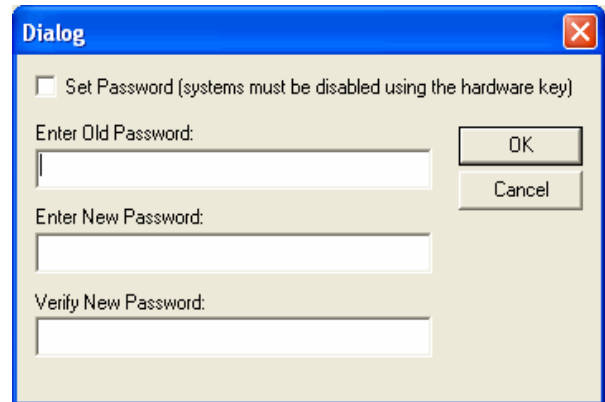
(Fig. 3.1.2)

Changing the Password - All Clients

1. Select **Set/Change Password** from the **Network Control** drop-down menu. (Fig. 3.5.0)
2. Enter the current password in the space provided. (Fig. 3.5.1)
3. Enter and Verify a new password. Select **OK** when finished.



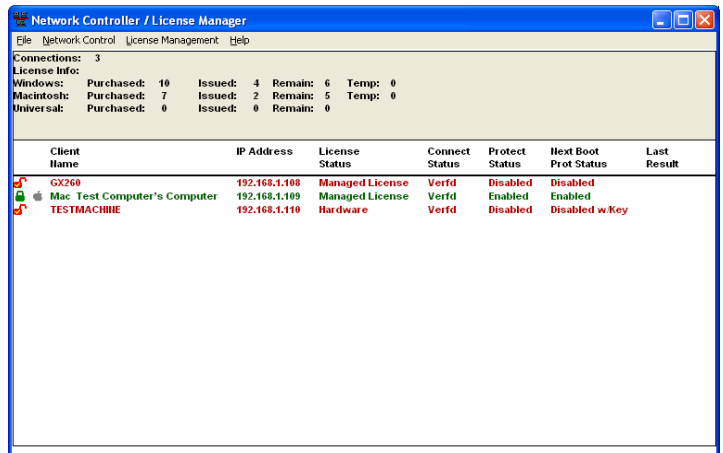
(Fig. 3.5.0)



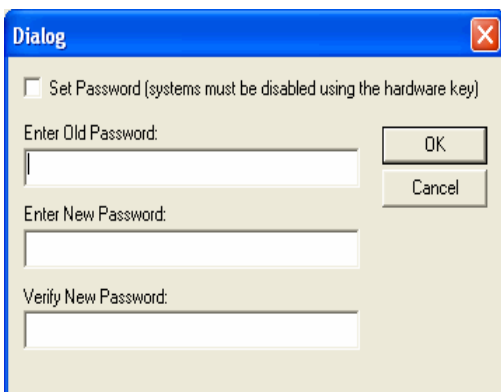
(Fig. 3.5.1)

Changing the Password - Individual Clients

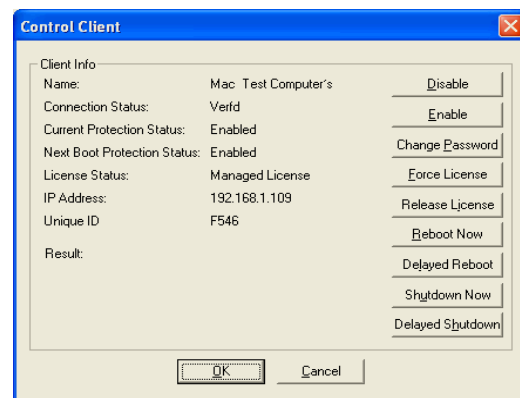
1. Double-click on the client of interest. (Fig 3.6.0)
2. Click the **Change Password** button. (Fig 3.6.1)
3. Enter the current password. (Fig 3.6.2)
3. Enter and verify a new password that will be used to disable the protection. Select **OK**. (Fig 3.6.2)
4. Now, select either **Reboot Now** or **Delayed Reboot** to reboot the system for the changes to take effect. (Fig 3.6.2)



(Fig. 3.6.0)



(Fig. 3.6.2)



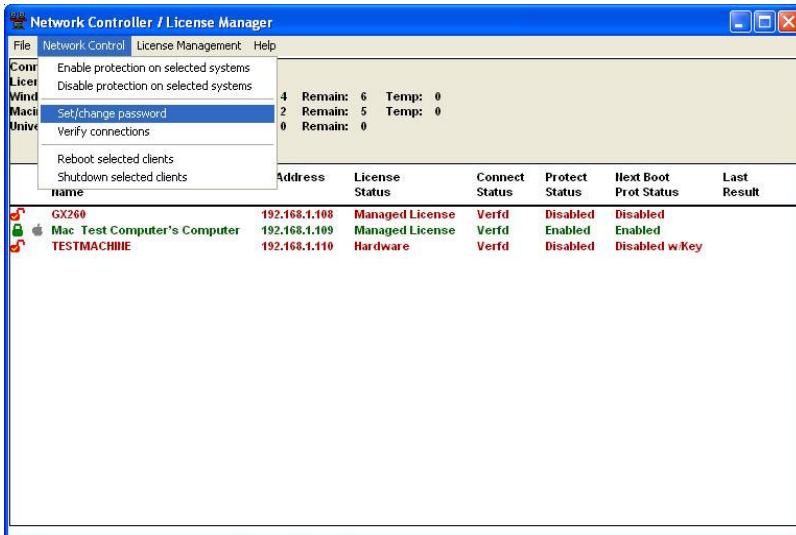
(Fig. 3.6.1)

Setting the Password - Centurion Guard - All Clients

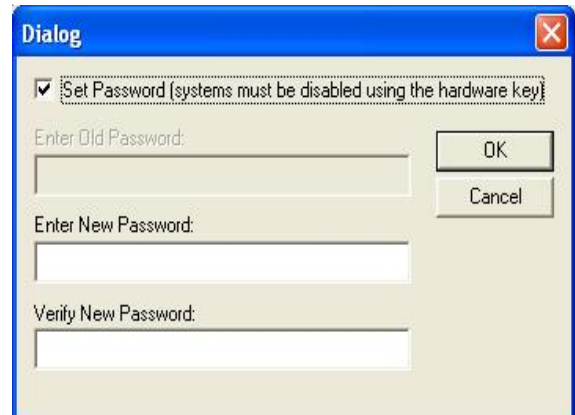
In order to remotely enable/disable the Centurion Guard, it is necessary to first set the password.

1. Select **Set/Change Password** from the **Network Control** drop-down menu. (Fig 3.7.0)
2. Click the check box at the top of the dialog next to **Set Password**. (Fig 3.7.1)
3. Enter and verify a password that will be used to disable the protection. Select **OK**. (Fig 3.7.1)

Note: To set the password, the key has to be in the disabled position.



(Fig 3.7.0)

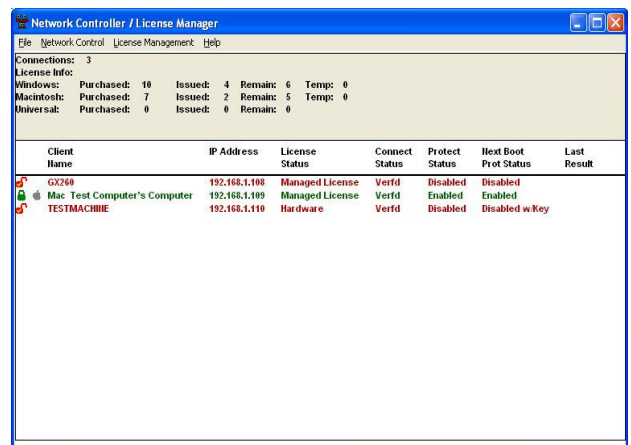


(Fig 3.7.1)

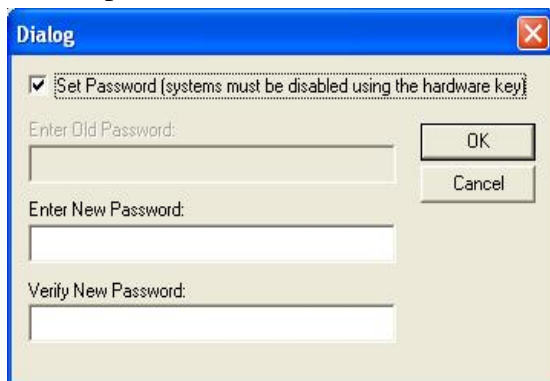
Setting the Password - Centurion Guard - Individual Clients

1. Double-click on the client of interest. (Fig 3.8.1)
2. Click the **Set Password** button. (Fig 3.8.2)
3. Enter and verify a password that will be used to disable the protection. Select **OK**. (Fig 3.8.2)
4. Now, select either **Reboot Now** or **Delayed Reboot** to reboot the system for the changes to take effect. (Fig 3.8.0)

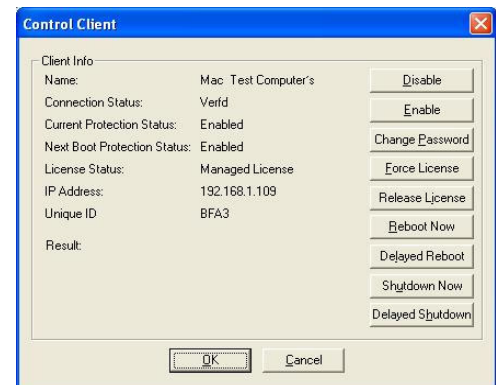
Note: To set the password, it is necessary for the key to be in the disabled position.



(Fig 3.8.1)



(Fig 3.8.2)



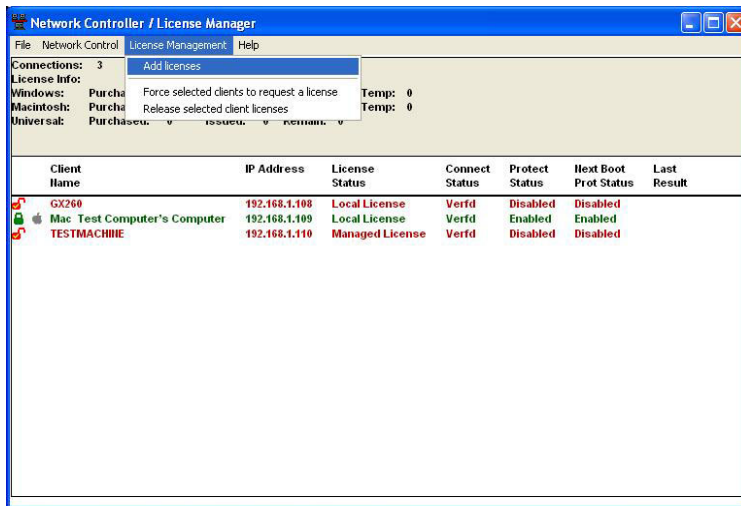
(Fig 3.8.0)

License Manager - Adding Licenses

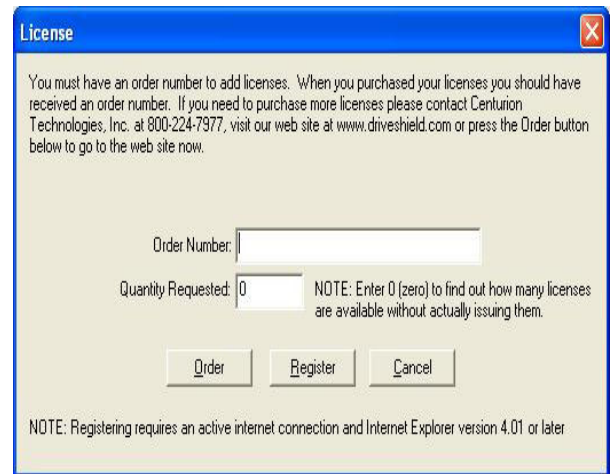
1. Select **Add Licenses** from the **License Manager** drop-down menu. (Fig 3.9.0)
2. A dialog will appear like the one below. Enter your Order Number and the Quantity of workstations you wish to register and select the **Register** button (Please note that you do not have to use all of your licenses right away. You may register a portion now and the others at a different time.) If you are uncertain of the quantity that was purchased or would like to know how many licenses are still available, enter **0** (zero) and select the **Register** button to find out. (Fig 3.9.1)

Note: If you do not yet have an Order Number you can select the **Order** button to place a purchase on-line or call (800)224-7977. Fig (3.9.1)

3. After you have successfully added licenses, the *Purchased* field will indicate the amount that has been added.



(Fig 3.9.0)

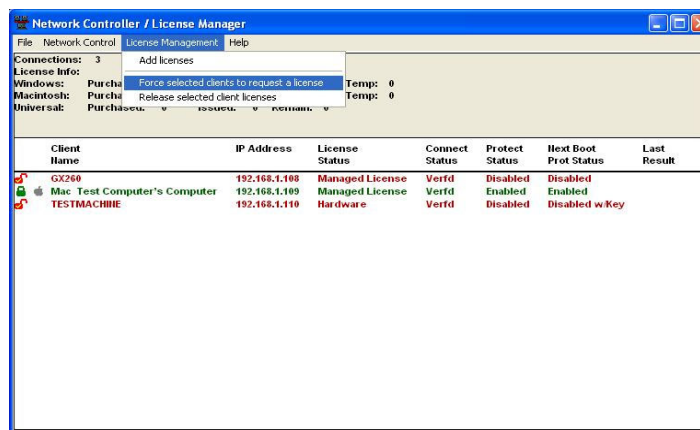


(Fig 3.9.1)

License Manager - Issuing Licenses

1. After you have successfully added licenses, you can begin issuing licenses to the workstations.
2. DriveShield software will not request a license if it is within the 30-day trial period. To force the systems to request a license from the server, select **Force All Clients to Request a License** from the **License Management** drop-down menu. The server will issue licenses to the workstations even if they are still in the trial period. Otherwise, after the trial period has ended DriveShield will automatically request a license from the License Manager. (Fig 3.9.2)

Note: Once a license is issued, License Manager will retain hardware specific information about the workstation. This will allow the workstation to be re-imaged, re-loaded, etc. without having to re-register DriveShield.

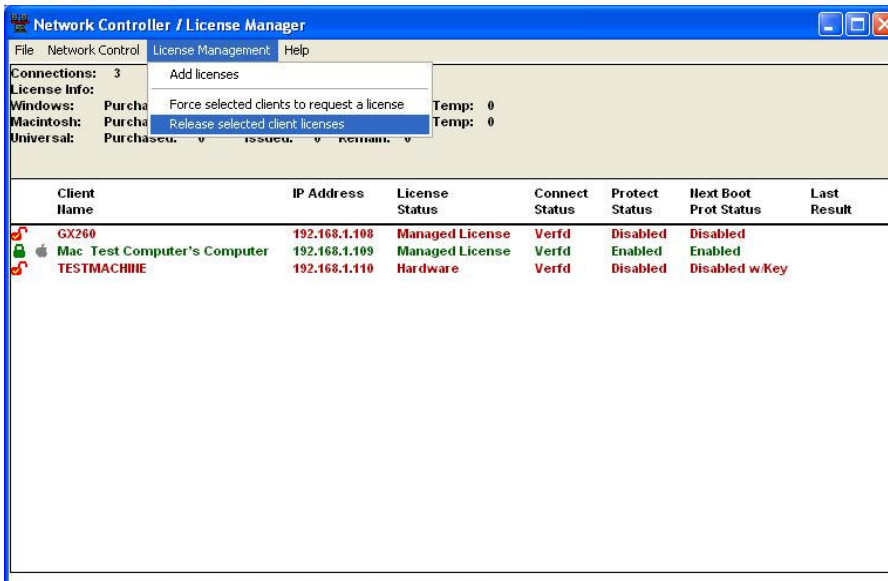


(Fig 3.9.2)

License Manager - Releasing Licenses

To transfer a license from one system to another you will need to, first, release the license from the registered machine. This will release the license from the client making available for issuance to another system. Please follow the instructions below to release a license.

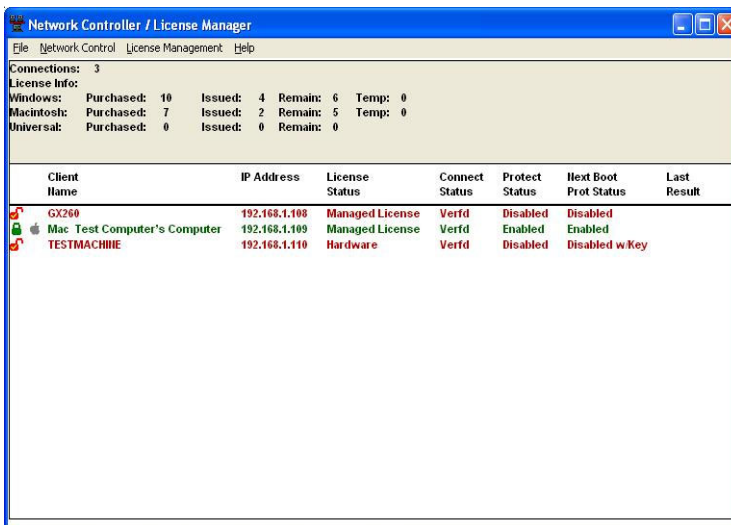
1. Select **Release All Client Licenses** from the **License Manager** drop-down menu. (Fig 3.9.3)
2. The **Remain** quantity will increase by the number of systems that are licensed and attached to License Manager. The **Issued** total will decrease by the quantity of systems that release their licenses.



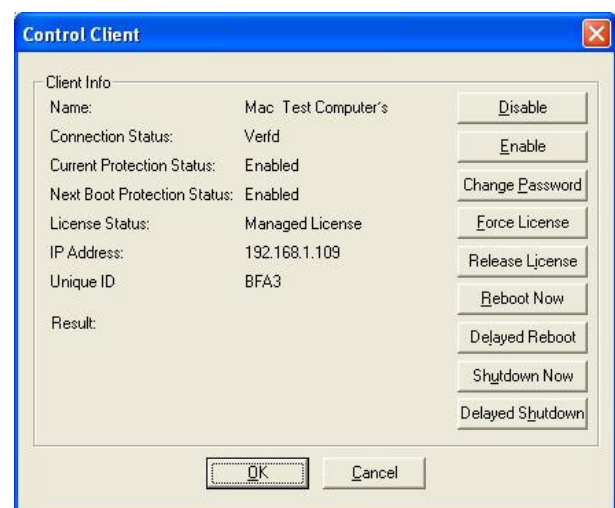
(Fig 3.9.3)

Releasing licenses can be done on an individual basis as well.

1. Double-click on the client system from which to release the license from. (Fig 3.9.4)
2. Click the **Release License** button to release the license. (Fig 3.9.5)



(Fig 3.9.4)



(Fig 3.9.5)

Network Controller - Options

Below is a list of the command line switches that are available for the Network Controller. In order to use these command line options, an instance of the NCLM server has to be running and the command has to be executed from the current NCLM program directory.

-e	<i>Enables the protection on all currently selected and connected systems.</i>
-d -pass:password	<i>Disables the protection on all currently selected and connected systems using password.</i>
-reboot	<i>Reboots all currently connected systems without delay.</i>
-delayedreboot	<i>Initiates a delayed reboot of all currently connected systems.</i>
-canceledelayedreboot	<i>Cancel a scheduled delayed reboot on all currently connected systems.</i>
-release	<i>Invalidates the licenses on all connected clients that the NCLM has issued and returns the licenses to the NCLM.</i>
-force	<i>Forces all clients to request a site license, even if they were already licensed.</i>
-shutdown	<i>Shutdown all currently connected systems without delay.</i>
-delayedshutdown	<i>Initiates a delayed reboot of all currently connected systems.</i>
-selectallclients	<i>Selects all currently connected systems.</i>

Command line examples:

```
ctictrl -d -pass:yourpassword
```

```
ctictrl -reboot
```

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior written permission of Centurion Technologies, Inc. Centurion Technologies, Inc. shall not be liable to the purchaser of this product or third parties for damages, losses, costs, or expenses incurred by purchaser or third parties as a result of: accident, misuse, or abuse of this product or unauthorized modifications, repairs, or alterations to this product.

General Notice: Other product names used herein are for identification purposes only and may be trademarks of their respective owners. Centurion Technologies, Inc. disclaims any and all rights in those marks.



Centurion Technologies, Inc.
512 Rudder Rd.
Fenton, MO 63026

(888) 265-6055 Technical Support
(800) 224-7977 Sales