

The Lock installation White Paper # 11000

This white paper covers installing The Lock in an Enterprise wide mixed system network. Covered items:

- a) Configuration of security for each Lock Security Zone, all from the PDC system.
- b) Deployment of remote Lock installations on client systems via Windows Logon scripts
- c) Deployment of remote Lock installations on client systems via TLNET utility (for systems not using a logon script)

Enterprise PC information:

Servers:

1 Windows 2003 Active Directory Primary Domain Controller

Domain Name: Test.ccstest.ccs.dom

Short Domain: TEST

Server Name: VPCWS2003

1 Novell Netware 5.0 NDS server

Server Name: CCNW5

Directory Tree: CCTR5

Workstations, broken down by department:

Management

05 Windows Vista Ultimate TEST domain member systems

10 Windows XP professional TEST domain member systems

05 Windows 2000 professional TEST domain member systems

Networking

05 Windows XP professional TEST domain member systems

Development

05 Windows Vista Business TEST domain member systems

05 Windows XP professional TEST domain member systems

05 Windows 2000 professional local install, networked systems

02 Windows 2000 professional TEST domain member systems

01 Windows ME TEST domain member systems

01 Windows 2000 professional CCTR5 member systems, also part of the TEST domain

01 Windows 98 professional CCTR5 member systems, also part of the TEST domain

QA

02 Windows Vista Ultimate TEST domain member systems

02 Windows Vista Business TEST domain member systems

02 Windows Vista Home Premium TEST domain member systems

10 Windows XP professional TEST domain member systems

02 Windows 2000 professional CCTR5 member systems, also part of the TEST domain

02 Windows 98 professional CCTR5 member systems, also part of the TEST domain

02 Windows 2000 professional TEST domain member systems

02 Windows ME TEST domain member systems

02 Windows 2000 local install, networked systems

02 Windows 98 local install, networked systems

Accounting (only Netware department in the enterprise. Authentication is still via TEST domain)

05 Windows 2000 professional CCTR5 member systems, also part of the TEST domain

05 Windows 98 professional CCTR5 member systems, also part of the TEST domain

Customer Support

50 Windows XP professional TEST domain member systems

25 Windows 2000 professional TEST domain member systems

Public Access (employee use PC's in the break area)

05 Windows XP Home systems

Zone configuration for The Lock

Zone 01: Primary security Zone. PDC (VPCWS2003) is the only system running in this zone.
Zone 30: Zone used for all Windows 98/ME systems logging into the TEST domain
Zone 31: Zone used for all Windows XP/2000/Vista systems logging into the TEST domain
Zone 32: Zone used for all Windows 98 systems logging into the CCTR5 NDS tree
Zone 33: Zone used for all Windows 2000 systems logging into the CCTR5 NDS tree
Zone 34: Zone used for all Windows 98 systems logging into the local system (not into the TEST domain)
Zone 35: Zone used for all Windows XP/2000/Vista systems logging into the local system (not into the TEST domain)
Zone 36: Zone used for all Windows XP/Vista Home systems

Network configuration for The Lock

The PDC has a folder created on C:\ called Public. The public folder has a folder called "TheLock", which contains three subfolders called: Images, Installs and Transfer. Your setup can be different, as the C:\Public folder tree is simply for example. The Zone folders from above are all stored in the C:\Public\TheLock\Images folder. The Auto Installer files are stored under the Transfer folder. For simplicity, I have downloaded the latest installs (thelock.zip and thelock_sms.zip) from the CrashCourse Software website, and saved them to the C:\Public\TheLock\Installs folder.

On the network, the C:\Public folder is shared with Everyone having Read access to the folder, and it's sub-folders, and with Administrators having full control.

Configuration Steps for The Lock Enterprise wide deployment

- 1) Install and configure The Lock on the PDC
- 2) Install and configure The Lock Security Manager Server (SMS) on the PDC
- 3) Configure all Windows 98/ME based security zones
- 4) Configure all Windows XP/2000/Vista Business/Ultimate* based security zones
- 5) Configure all Windows XP/Vista Home based security zones
- 6) Configure all newly created Zones in the SMS configuration utility
- 7) Export SMS auto installers for each newly created Zone.
- 8) Create Cloned Images
- 9) Modify client logon scripts to automatically deploy The Lock on the client system upon logon
- 10) Launch SMS Auto Installer on Vista Ultimate/Business* and /XP/Vista home systems to deploy The Lock

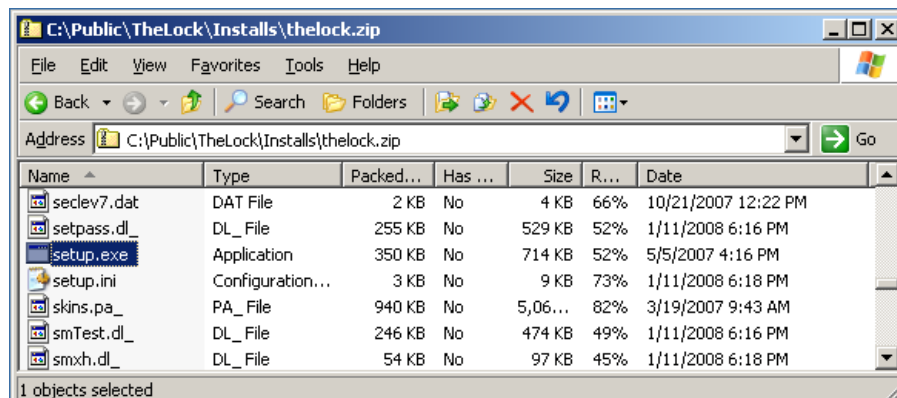
* When UAC is enabled, Windows Vista requires installation by an Administrator via the SMS Auto Installer run at the workstation. If installation via the logon script is preferred, NETLOCK will launch, and the user at the remote system will be presented with the UAC dialog stating that NETLOCK is requesting Administrative access to the system. Upon the users selection of the Allow option, The Lock will be installed as normal.

Without UAC enabled, Windows Vista installations are accomplished the same way as Windows XP/2000 systems via the logon script.

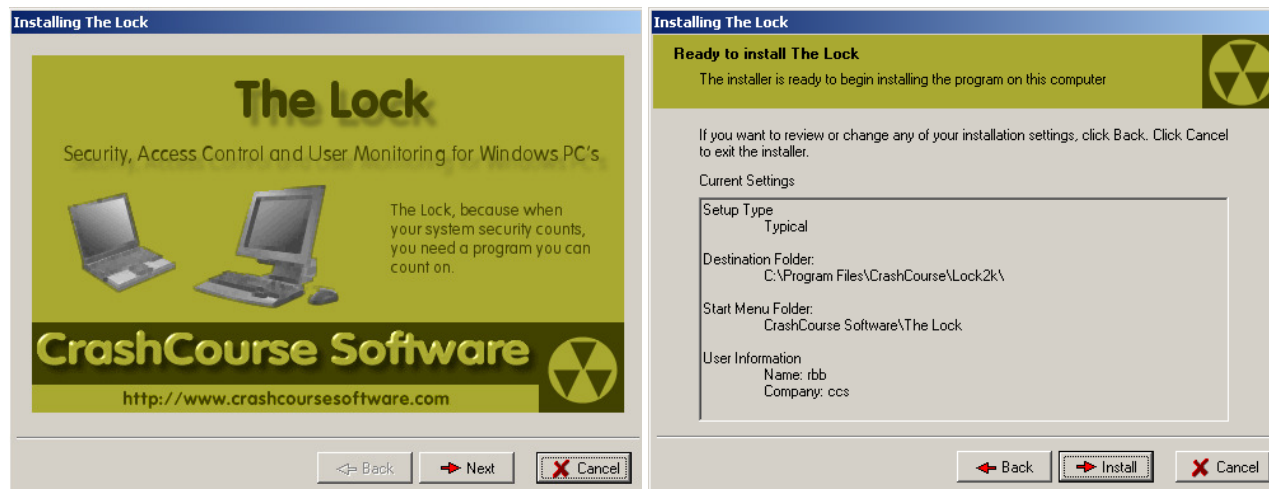
In all cases, user interaction, either end user or Administrator, is only required during initial installation on a system that does not already contain a Vista compatible version of The Lock.

Section 1: Installing The Lock on the PDC system

Download and save The Lock's ZIP file to a folder on the PDC. As is shown in the following image, "thelock.zip" has been saved to the "C:\Public\TheLock\Installs folder."



Double clicking on "setup.exe" will start the installer. Default settings were selected during the installation.



When the image on the right hand side appears, click the Install button to install The Lock on the system. When installation is complete, a dialog will appear as follows:



In order to enable full security on the system, you will need to select Yes at this dialog.

Click the Finish button when the "Installation Complete" page appears. This will start the next phase of the installation process.

Configuration of The Lock, Zone 1, on the PDC

Once setup begins, a prompt will appear that will allow you to view the Quick Start Guide, in the case of this white paper, this step is not needed, so “No” is selected.

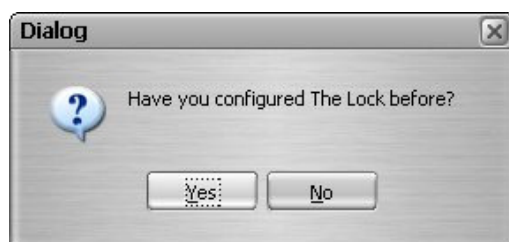
The Lock Configuration Utility will load next, and the following dialog will be displayed:



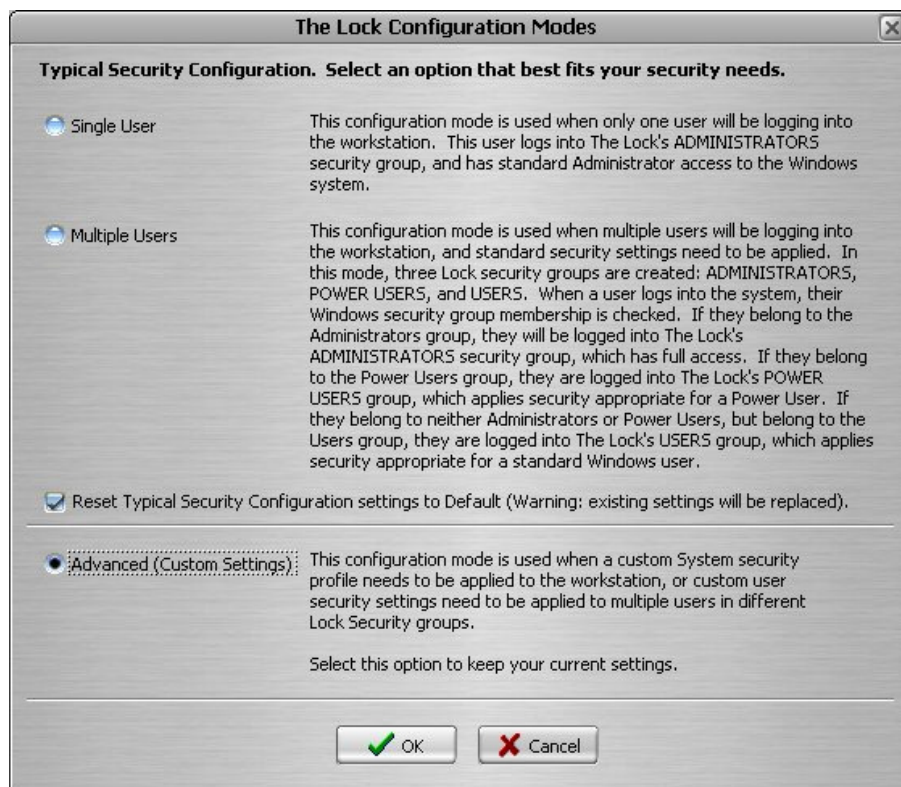
The next dialog is very important, as it will configure The Lock’s Master Administrator password. This password is needed to access the system when booted in Safe Mode, as well as logging into any users session, without having to log them out first. It is also used during uninstall, and must be entered before The Lock can be removed.

If you have logged into Windows with an account not named Administrator, you will be prompted that a Lock User has been created in the Administrators group with the same name you logged in under.

The next dialog will ask if you have configured The Lock before, select yes.



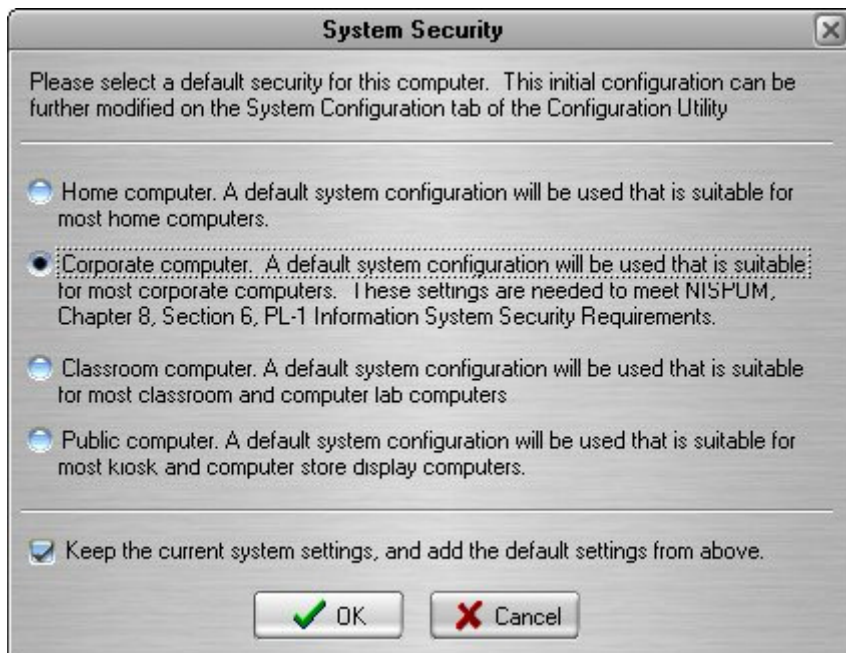
Keep the default selections [Advanced (Custom Settings)] on “The Lock Configuration Modes” dialog, and click OK:



The next dialog will ask if you would like to run The Lock's Setup Configuration Wizard:



No was selected, and the following dialog was displayed.

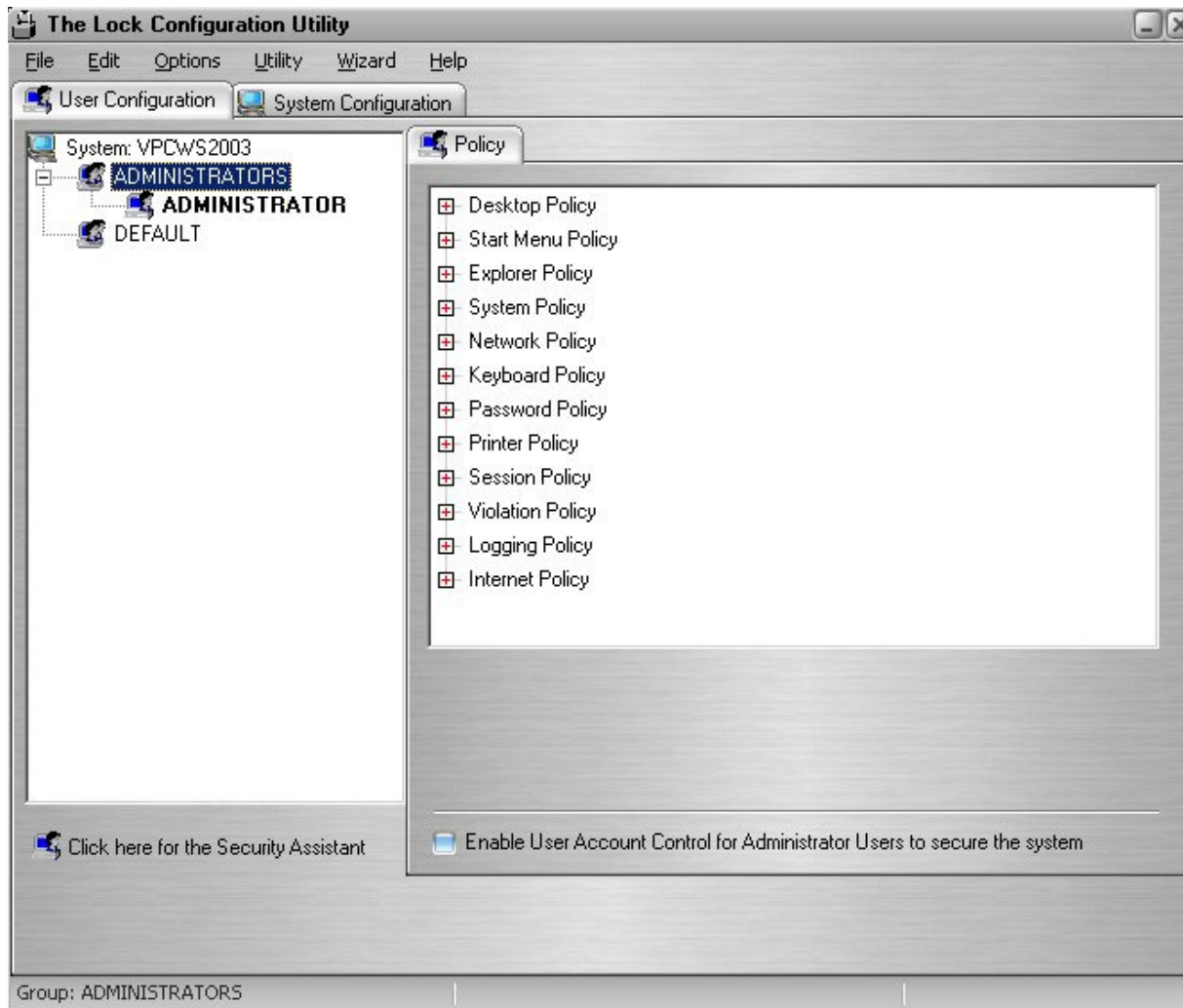


Since this system is the PDC, and only the Administrator will have access to it, I have selected the "Cancel" button on this dialog.

The next dialog will prompt asking if you would like to have the Security Assistant help you set your basic system configuration. Click "No".

The next dialog will be a prompt stating that The Lock has discovered Windows users, and would like to import them. Select "No" to this dialog. Finally, select No to the "Would you like to create any new users now?" dialog.

Initial setup of The Lock is now complete, and you should see the following window:



Initial configuration for The Lock, on the PDC, in Zone 1, is now complete. Select File, then Exit, to continue.

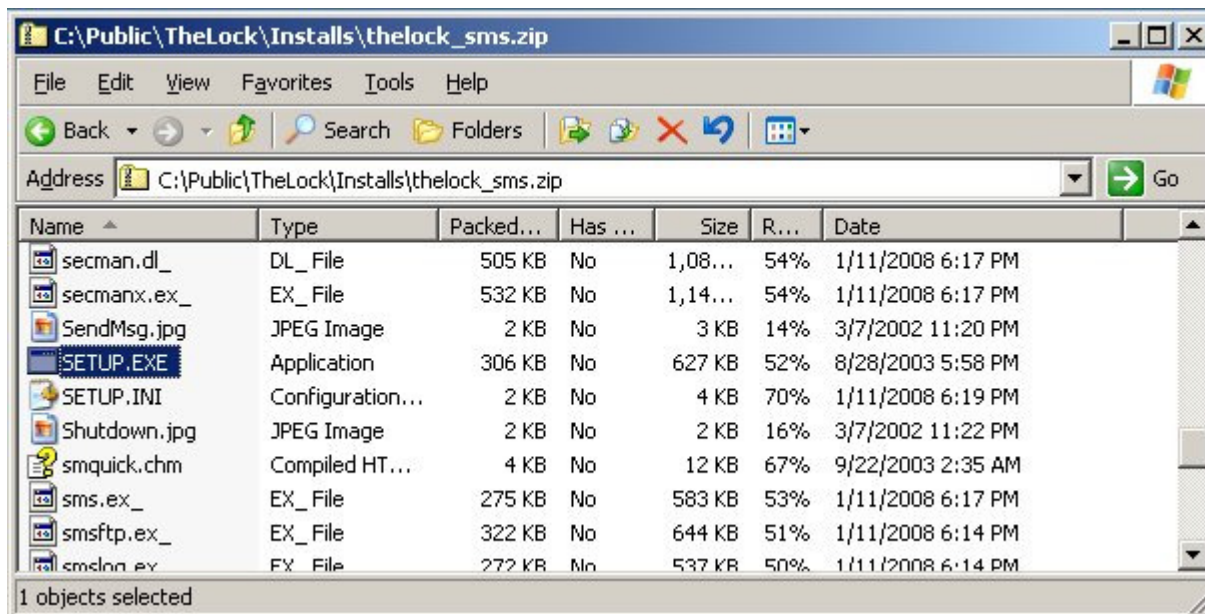
The following prompts will now appear:

- 1) Would you like to enter your registration information now? Select Yes if you have this information, or select No if you are running the program in Demo mode.
- 2) Would you like The Lock to load each time Windows starts (recommended). Select Yes to have The Lock run automatically each time the system is started.
- 3) Would you like The Lock to secure Safe Mode access to the system? Select Yes for maximum security.
- 4) Once The Lock is loaded, and a user has logged in, would you like to automatically lock the system (display The Lock's password dialog)? Setting this option will require the user to type their password for Windows, then type their password for The Lock before they will be able to access the Windows Desktop. Select No here, unless you want to have to type your password again, before access to the Desktop is allowed.
- 5) Would you like to create an Administrator key disk now (recommended)? Click Yes here.
- 6) This option will create an emergency access key disk. Place a 3.5 inch floppy disk into drive A: and press OK. (Press and hold Shift to create the emergency file in the C:\Temp\ folder for use on a CD-R, ZIP disk, or USB Thumb Drive instead of a floppy.) Press and hold Shift, then click OK.
- 7) An emergency access file was successfully created at "C:\Temp\Command.old". Take this file, and move it to the root of any type of removable media.
- 8) Would you like to restart your computer before using The Lock (recommended)? Click Yes here.

Configuration of The Lock, Zone 1, on the PDC is now complete, but you may have to manually restart the system.

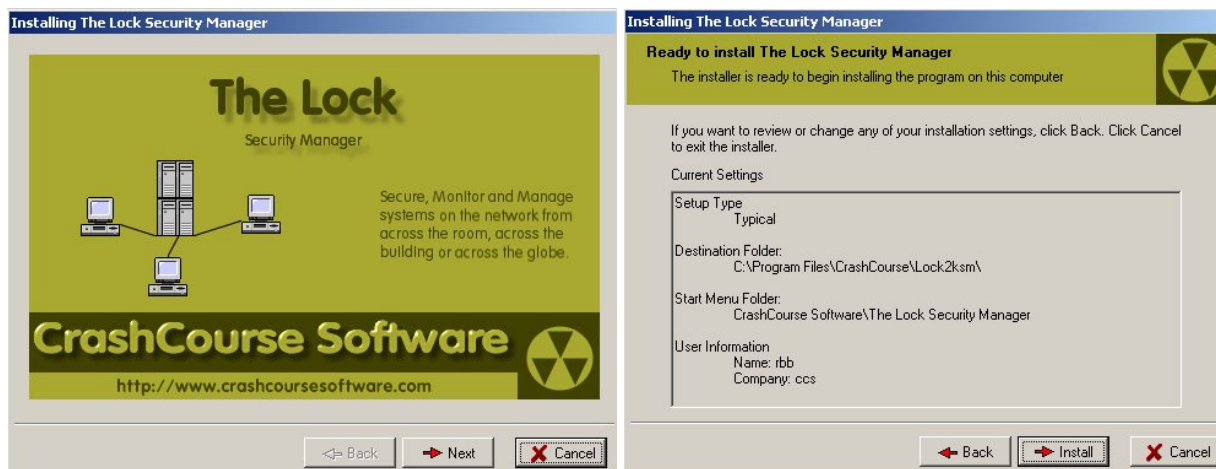
Section 2: Installing The Lock Security Manager Server (SMS) on the PDC system

Download and save The Lock Security Manager Server's ZIP file to a folder on the PDC. As is shown in the following image, "thelock_sms.zip" has been saved to the "C:\Public\TheLock\Installs" folder.



Double clicking on "setup.exe" will start the installer.

If The Lock is running (as it is now), you will be prompted to exit The Lock before setup can continue. Click the OK button to continue. Right click The Lock's padlock icon, in the system tray, and select Security, then Exit. Type the Master Administrator password to exit the program. Double click the "setup.exe" program again.

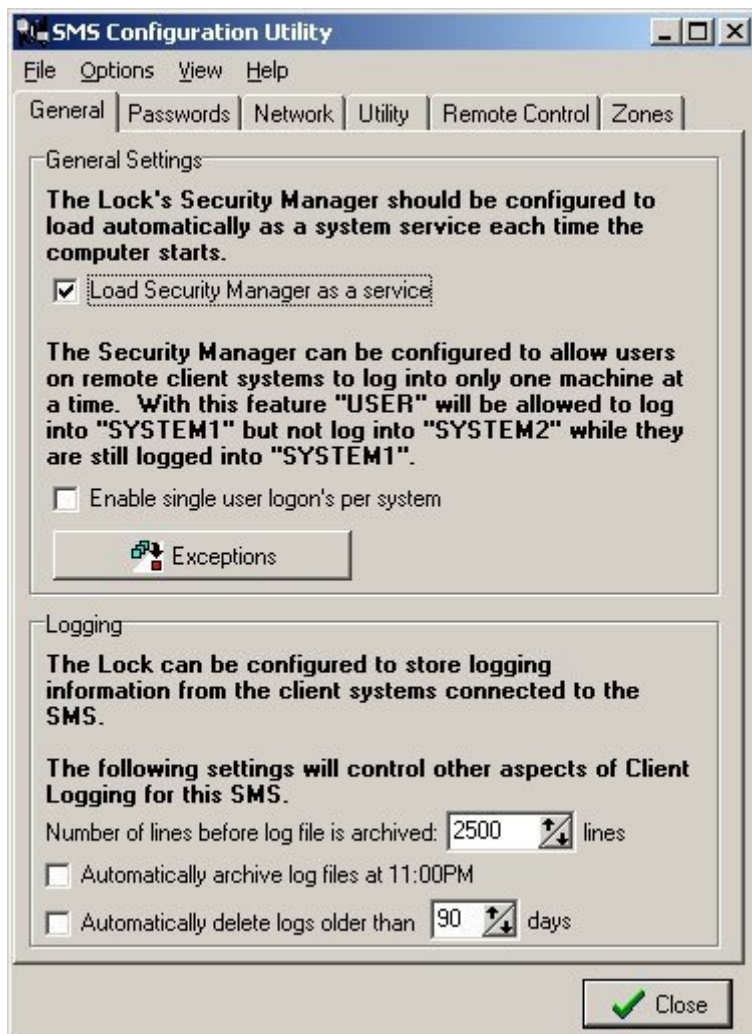


Default settings were selected during the installation. After clicking "Install", the SMS will be installed on the system. Once installation is complete, press the "Finish" button to exit the setup utility; the Security Manager Server will start automatically.

When the SMS starts, it will prompt to view the Security Manager Quick Start Guide, select No.

The SMS will now load the Configuration Utility. You will need to set two options on the General tab.

- 1) Check the option to "Load Security Manger as a service"
The settings for the General tab now look like this:



- 2) Select the Zones tab.
- 3) In the Primary Cloned Image Folder (Zone 1) edit box add: C:\Public\TheLock\Images\Zone01\
- 4) Select the Network tab.
- 5) Put a check mark in the "Enable Web Interface" box, then click Set for the "Web interface password". Set this password to what ever you like, but keep in mind, it will be used to access the SMS Web Interface.
- 6) Set your "client-Server Data Communications" user name and password. You do not need to perform this step for the SMS too work properly, but we recommend this User Name and Password to be changed. In this white paper, we will be using a user name of "locftp" and a password of "locpass".
- 7) Click the Close button to exit the SMS Configuration Utility, selecting Yes to save new settings.

There is only one more step to complete before we can connect to the SMS from a Lock client. Press the Start Menu, select All Programs, then CrashCourse Software, then The Lock, then select the icon for The Lock.

Once The Lock is started, right click the padlock icon in the system tray, select Settings, then Configuration Utility. Type the Master Administrator password, and the Configuration Utility will start.

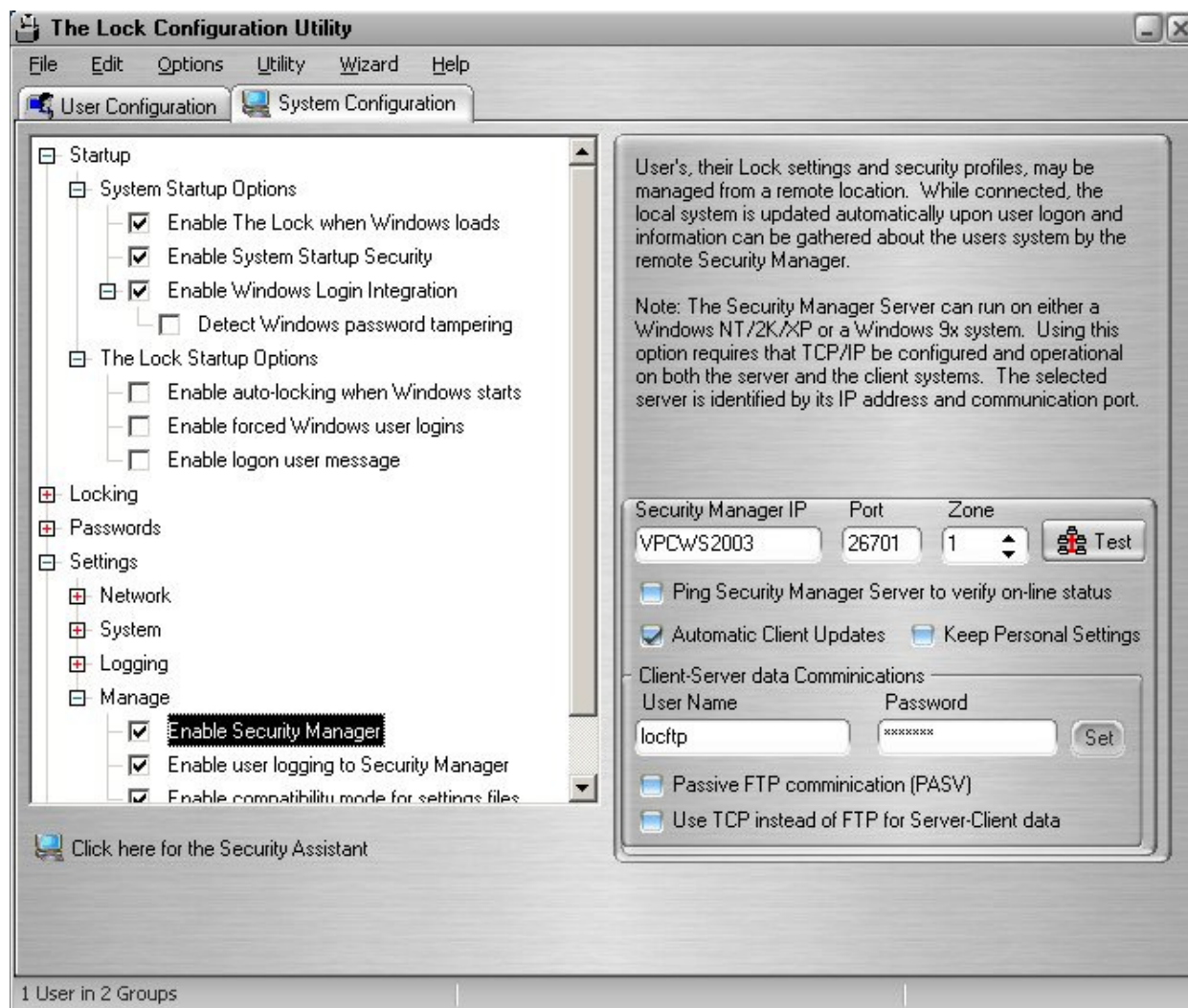
Once the Configuration Utility has started, click Close on the Tip of the Day (if it appears), then select the System Configuration tab.

Expand the Settings branch, then the Manage branch. Highlight the "Enable Security Manager" item, and place a check mark in the box.

In the right hand window, set the Security Manger IP to "VPCWS2003" (or the name of your PDC server), and click test. You should get a message stating that a Security Manager Server has been found.

The Lock will now be able to communicate with the SMS that was just installed.

Next, place a check box for the item "Enable user logging to Security Manager", if you prefer to have your user logs in a centralized location. When you highlight the "Enable Security Manager" option again, your window should look like this:



Security Zone 1 (as shown above) is now completely configured.

You will now save the current configuration as the Zone 1 (or default) security zone by following this procedure:

- 1) On the Configuration Utility's main menu, select File, then Export, then "User and System Configuration to a file".
- 2) If prompted, select Yes to save new settings.
- 3) On the save dialog, browse to C:\Public\TheLock



- 4) If it does not exist, add a new folder called Images by pressing the folder with the red + sign on it. (
- 5) Name the folder Images, click off of it, then double click it.
- 6) If it does not exist, add a new folder called Zone01, click off it, then double click it.
- 7) Change the save file name to netlock.cfg, then click Save. A dialog will appear when settings have been saved

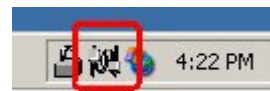
You may now close the Configuration Utility; you will be prompted to save settings, select Yes. You may be prompted to add the updated settings to the current cloned image, Select No.


When you are returned to Explorer, restart the computer.

Sections 3 – 5: Configuring Zone based Security

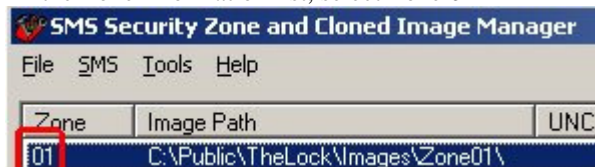
Creating Zone 30 for all Windows 98/ME systems logging into the TEST domain.

Zone notes: This is the basic, Windows 9x/ME based Zone configuration in this enterprise. This security zone is primarily used by the Development and QA departments.



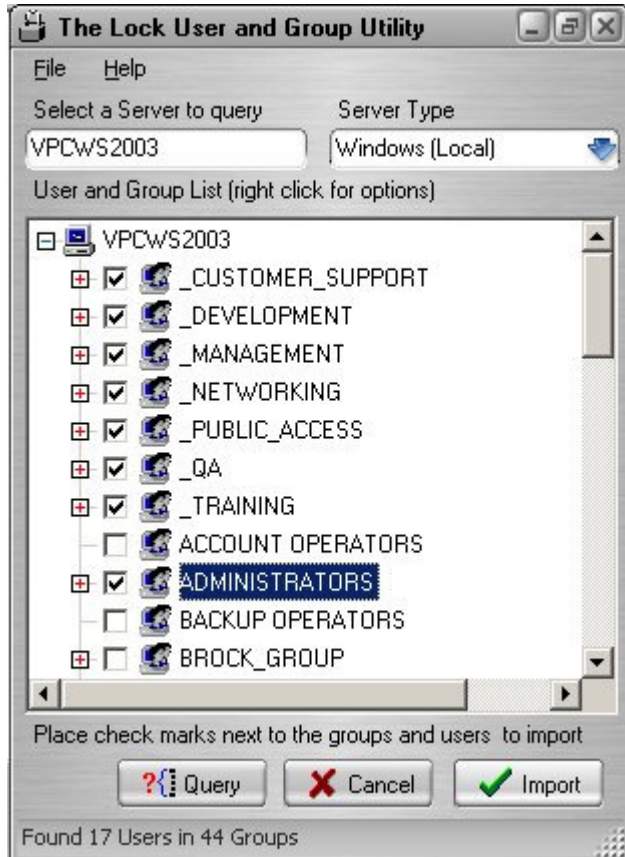
Open The Lock SMS Configuration Utility by right clicking the icon in the system tray () and selecting SMS Configuration Utility:

- 1) If prompted, enter the Master Administrator password
- 2) Select the Zones tab
- 3) Click the “Edit Zone Information” button
 - a. On the SMS Security Zone and Cloned Image Manager , Select the Local SMS Security Zone Data Path entry and set it to: C:\Public\TheLock\Images
 - b. Select the UNC SMS Security Zone Data Path entry and set it to: \\VPCWS2003\Public\TheLock\Images
 - c. In the Zone information list, select Zone 01



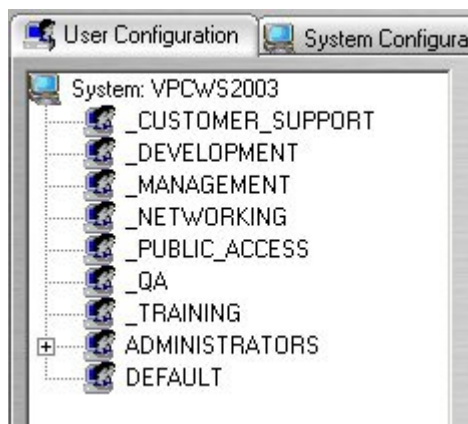
- d. From the menu, select SMS then “Duplicate selected SMS Security Zone”
 - e. Type a new security zone called 30, click OK.
 - f. On the SMS Security Zone Configuration dialog, set:
 - g. The local image path to: C:\Public\TheLock\Images\Zone30\
 - h. Set the UNC path to \\VPCWS2003\Public\TheLock\Images\Zone30\
 - i. Set the Description to “Windows 98/ME Systems on the TEST domain”
 - j. Click OK
 - k. A dialog will appear asking to configure settings for the new security zone. Click Yes
- 4) The Lock Configuration Utility will open, and configuration for Security Zone 30 can begin.
- 5) Select the “System Configuration” tab
- 6) Select Options, then Set default system security
- 7) On the system security tab, take the default of “Corporate computer”
- 8) Click OK
- 9) Select the “Enable logon user message” under the “The Lock Startup Options” branch
- 10) In the right hand window, check the option “User message is automatically canceled after 20 seconds”
- 11) Next, Expand the Passwords branch
- 12) Expand the Authentication branch
- 13) Check the option for Use Windows Server password
- 14) Next, Expand the Settings branch,
- 15) Expand the Network branch
- 16) Select the “Enable Network Group Synchronization” item and place a check mark in the box.
- 1) In the right hand window, Change the “Users in this group are read from the group list on” drop down to “an Active Directory Server”
- 17) Next, select the “Enable settings update on startup” option, and make sure it is un-checked.
- 18) Next, Expand the Logging branch
- 19) Uncheck the options for “Include Security Event Log entries” and “Local audit policy”
- 20) Next, Expand the Manage branch
- 21) Select Enable Security manager
- 22) Verify the Zone entry is set to 30
- 23) Click the User Configuration tab, at the top of the Configuration Utility
- 24) Select the File Menu, then Import, then Users and Groups, then Network Server.
- 25) In The Lock User and Group Utility, type the name of the PDC as the Server to query, or simply double click the edit box to set the value automatically
- 26) Press the Query button, and the users and groups will be read from the local windows system.

- 27) As part of my initial PDC setup, I created custom Windows groups for all enterprise departments. Each group I created has a leading underscore, so that they will be listed at the start of any group lists.
- 28) Before pressing the Import button, uncheck any group name that does not have a leading Underscore, except for the Administrators group, and uncheck all user names, if desired. Since this Zone is configured to allow users based on their Windows Server group membership, all we need to import is the group names themselves. Users may be all checked or all unchecked using the right click context menu
- 29) The window will now look like this:



- 30) Click Import

The user list in The Lock now looks like this:



- 31) Since the Management, Networking, Customer Support, and Public Access departments do not run Windows 9X machines, we can remove those groups from the User and Group list. Since the Training department Windows 98 machines log into Netware servers, we can remove the Training group as well.

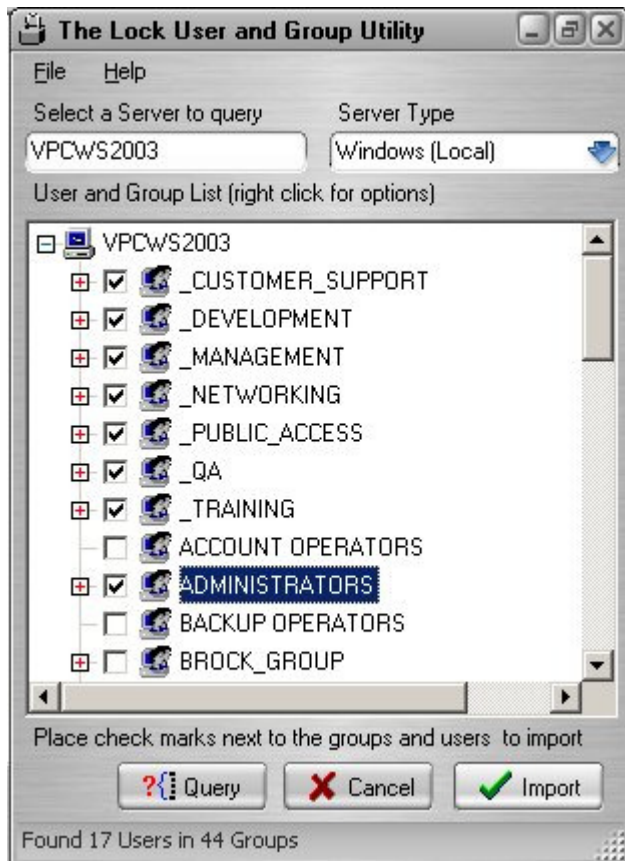
- 32) We are now left with four security groups: _DEVELOPMENT, _QA, ADMINISTRATORS and DEFAULT. The DEFAULT security group is not used in this Zone, and the ADMINISTRATORS group is only used by the Administrator, and any users who is a primary member of the Windows Administrators security group.
- 33) We will now configure Group security for this Zone.
 - a. As this enterprise setup is for a corporation, each group will have a basic minimum default group security level. The exception to this rule is the _DEVELOPERS group, as users in this group will need to have some Administrative access to the system. The groups will be configured one at a time, starting with the _DEVELOPMENT group.
 - b. Right click the _DEVELOPMENT security group, and select “Set Default Group Security”.
 - c. Select the option “This group has Corporate restrictions”
 - d. Click OK.
 - e. On the Policy Tab, expand the “System Policy” branch.
 - i. Uncheck “Disable Access to Administration tools”
 - ii. Uncheck “Disable Registry Editor”
 - iii. Uncheck “Disable Task Manager”
 - iv. Uncheck “Disable System Properties Control Panel”
 - v. Uncheck “Secure Registry Run Keys”
 - f. Select the File System tab
 - g. Remove the following entries from the File and Folder Security list: ATTRIB.EXE (NA), DELTREE.EXE (NA), EDIT.COM (NA), SUBST.EXE (NA), XCOPY.EXE (NA), and XCOPY32.EXE (NA)
 - h. The _DEVELOPMENT security group is now configured. Select the group name (if it is not already), select the “Options” menu, then “Groups”, then “Export security settings from this group”
 - i. If the Save As dialog is not already pointing to C:\Public\TheLock\Settings, browse there, then click the Save button. The file name will default to the group name. With this group’s settings saved, we will be able to re-use them when configuring the other Security Zones.
- 34) We will now configure Group security for the _QA group.
 - a. We will start out by setting the default security, so right click _QA, and select “Set Default Group Security”.
 - b. Select the option “This group has Corporate restrictions”
 - c. Click OK.
 - d. Our QA department only operates from 6:00am to 6:00pm, so time restrictions need to be added. Select the Times tab.
 - i. Highlight all times before 6:00am, right click and select “Deny Login”
 - ii. Highlight all times after 6:00pm, right click and select “Deny Login”
 - e. This group will also not have access to the Developers folder, which resides at C:\Dev on all Development and QA systems.
 - i. Add the C:\Dev folder as restricted by selecting the File System tab
 - ii. On the File and Folder Security sub-tab, click the Add button.
 - iii. Add the entry for the folder name as C:\Dev
 - iv. Put a mark in the No Access check box
 - v. Click OK
 - f. The _QA security group is now configured. Select the group name (if it is not already), select the “Options” menu, then “Groups”, then “Export security settings from this group”
 - g. If the Save As dialog is not already pointing to C:\Public\TheLock\Settings, browse there, then click the Save button. The file name will default to the group name. With this group’s settings saved, we will be able to re-use them when configuring the other Security Zones.
- 35) Zone 30 is now configured. Select the File menu, then Exit.
- 36) You may be prompted to query users from an AD server, select No.
- 37) You will be prompted that “Settings have been changed, save new settings?”, select Yes.
- 38) You will be prompted to “Add the updated settings to the Zone 30 cloned image”, select Yes.
- 39) Security Zone 30 is now configured and added to the “SMS Security Zone and Cloned Image Manager”

Creating Zone 31 for all Windows 2000/XP/Vista systems logging into the TEST domain.

Zone notes: This is the basic, Windows NT based Zone configuration in this enterprise. This security Zone contains group information that will allow any user in the enterprise to log into their computer.

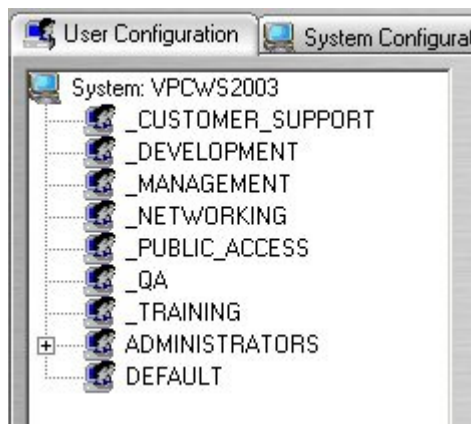
- 1) Create a new security zone
- 2) On the SMS Security Zone and Cloned Image Manager, select Zone 01
- 3) From the menu, select SMS then “Duplicate selected SMS Security Zone”
- 4) Type a new security zone called 31, click OK.
- 5) On the SMS Security Zone Configuration dialog, set:
 - 6) The local image path to: C:\Public\TheLock\Images\Zone31\
 - 7) Set the UNC path to \\VPCWS2003\Public\TheLock\Images\Zone31\
 - 8) Set the Description to “Windows 2000/XP/Vista Systems on the TEST domain”
- 9) Click OK
- 10) A dialog will appear asking to configure settings for the new security zone. Click Yes
- 11) The Lock Configuration Utility will open, and configuration for Security Zone 30 can begin.
- 12) Select the “System Configuration” tab
- 13) Select Options, then Set default system security
- 14) On the system security tab, take the default of “Corporate computer”
- 15) Click OK
- 16) Select the “Enable logon user message” under the “The Lock Startup Options” branch
- 17) In the right hand window, check the option “User message is automatically canceled after 20 seconds”
- 18) Next, Expand the Passwords branch
- 19) Expand the Authentication branch
- 20) Check the option for Use Windows Server password
- 21) Next, Expand the Settings branch,
- 22) Expand the Network branch
- 23) Select the “Enable Network Group Synchronization” item and place a check mark in the box.
- 24) In the right hand window, click the drop-down list, and select “an Active Directory Server”
- 25) Next, Expand the Logging branch
- 26) Check mark the options for “Include Security Event Log entries” and “Local audit policy”
- 27) Next, Expand the Manage branch
- 28) Select Enable Security manager
- 29) Ensure the Zone entry is set to 31
- 30) Click the User Configuration tab, at the top of the Configuration Utility
- 31) Select the File Menu, then Import, then Users and Groups, then Network Server.
- 32) In The Lock User and Group Utility, type the name of the PDC as the Server to query, or simply double click the edit box to set the value automatically
- 33) Press the Query button, and the users and groups will be read from the local windows system.
- 34) Before pressing the Import button, uncheck any group name that does not have a leading Underscore, except for the Administrators group, and uncheck all user names, if desired. Since this Zone is configured to allow users based on their Windows Server group membership, all we need to import is the group names themselves.

35) The window will now look like this:



36) Press Import to import the selected groups.

37) The user list in The Lock now looks like this:



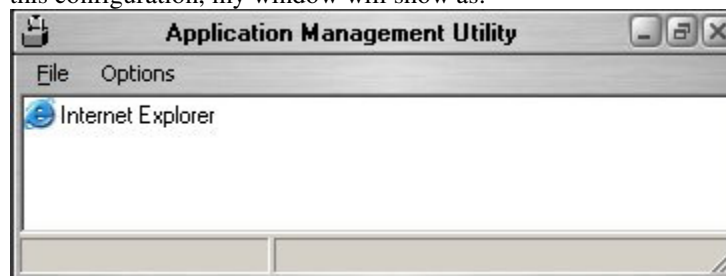
38) Since All departments run at least one Windows XP, Windows 2000, or Windows Vista system, we will leave each group in the list.

- 39) We will now configure Group security for this Zone.
- a. As this enterprise setup is for a corporation, each group will have a basic minimum default group security level. The exception to this rule is the `_DEVELOPERS` group, as users in this group will need to have some Administrative access to the system. The groups will be configured one at a time, starting with the `_DEVELOPMENT` group.
 - b. Right click the `_CUSTOMER_SUPPORT` security group, and select “Set Default Group Security”.
 - c. Select the option “This group has Corporate restrictions”
 - d. Click OK.
 - e. Since this is an elevated restriction group, we will set some extra security settings now.
 - f. On the Policy Tab, expand the “Desktop Policy” branch. Check mark the following options, leaving any existing settings as they are
 - i. “Disable Desktop Drag and Drop”
 - ii. “Lock Desktop Icons”
 - iii. “Disable Display Properties Control Panel”
 - iv. “Disable Background tab in the Display control Panel”
 - g. Expand the “Start Menu Policy” branch. Check mark the following options, leaving any existing settings as they are
 - i. “Disable changing the Windows Start Menu”
 - ii. “Disable Settings option on the Windows Start Menu”
 - iii. “Disable Taskbar option on the Windows Start Menu”
 - h. Expand the “Explorer Policy” branch. Check mark the following options, leaving any existing settings as they are
 - i. “Disable Control Panel”
 - ii. “Disable Windows Help”
 - i. Expand the “System Policy” branch. Check mark the following options, leaving any existing settings as they are
 - i. “Disable viewing of Hidden and System files in Windows Explorer”
 - ii. “Disable Date/Time changes”
 - iii. “Disable installing Programs”
 - j. Expand the “Network Policy” branch. Check mark the following options, leaving any existing settings as they are
 - i. “Disable Network Properties Control Panel”
 - ii. “Disable Add/Remove Network share button”
 - iii. “Disable Network sharing controls”
 - k. Expand the “Keyboard Policy” branch. Check mark the following options, leaving any existing settings as they are
 - i. “Disable Print Screen Key”
 - ii. We only want the print screen key disabled in Internet Explorer, and further-more, we only want it disabled when in Internet Explorer, and on the CrashCourse Software website. We also want it disabled in Notepad, when an Untitled document is open. Double click the text “Configure Print Screen Key Restrictions”
 1. Change the radio button from the first item, to the second (“The Print Screen Key is restricted for Windows with the following titles:”
 2. Click the Capture button. You will be prompted with the key sequence to capture the information about the window.
 3. Open Internet explorer, browse to www.crashcoursesoftware.com, once the page loads, press the hot key noted in #2, above.
 4. Next, click Start, then Run, then type Notepad. Once Notepad loads, press the hot key again.
 5. Both entries are now in the Print Screen Key Configuration list. Click the End button, then click OK.
 - l. Expand the “Password Policy” branch. Check mark the following options, leaving any existing settings as they are
 - i. “Disable Changing Lock Password”
 - ii. “Disable Password Control Panel”
 - iii. “Disable Change Password Tab in Password Control Panel”
 - m. Expand the “Printer Policy” branch. Check mark the following options, leaving any existing settings as they are
 - i. “Disable Printer sharing controls”
 - ii. “Disable Add New Printer”
 - iii. “Disable Remove Printer”

- n. Expand the “Logging Policy” branch. Check mark the following options, leaving any existing settings as they are
 - i. “Enable URL Audit Logging”
 - o. Expand the “Internet Policy” branch. Check mark the following options, leaving any existing settings as they are
 - i. “Disable changing the Home and Search page in Internet Explorer”
 - ii. “Disable file download in Internet Explorer”
 - p. Our Customer Service department only operates 24 hours a day, so no time restrictions need to be added. Select the Times tab, and uncheck “Enable Login time restrictions based on the schedule above”
 - q. Select the File System tab, then add the following new items:
 - i. Click Add, then click the Drives button. Check mark the Floppy, then check mark “No Access”
 - ii. Click Add, then click the Drives button. Check mark the CD-ROM, then check mark “No Access”
 - iii. Click Add, then click the Drives button. Check mark the Removable, then check mark “No Access”
 - iv. Click Add, then click the Drives button. Check mark the System Disk, then check mark “Read Only”
 - v. Click Add, then click the Drives button. Check mark the Hard Disks, then check mark “Read Only”
 - vi. In the File and Folder Security list, select the entries for <RUNDIR>*.* (RO) and <WINDOWS>*.* (RO) and press the Remove button. These entries are redundant, as the System Disk entry above will automatically restrict both these entries.
 - r. Select the Programs tab.
 - i. Right click and select “Add Common”, then “Control Panels”, then “Add All”
 - ii. Right click and select “Add Common”, then “Other Programs”, then “Shell Settings”
 - iii. Right click and select “Add Common”, then “Other Programs”, then “System Tools”
 - s. The _CUSTOMER_SUPPORT security group is now configured. Select the group name (if it is not already), select the “Options” menu, then “Groups”, then “Export security settings from this group”
 - t. If the Save As dialog is not already pointing to C:\Public\TheLock\Settings, browse there, then click the Save button. The file name will default to the group name. With this group’s settings saved, we will be able to re-use them when configuring the other Security Zones.
- 40) We will now configure Group security for the _DEVELOPMENT group.
- a. Since we have already configured security for the _DEVELOPMENT group, it is already set. Otherwise, we would simply use our saved _DEVELOPMENT group settings by following this procedure:
 - b. Highlight the _DEVELOPMENT group
 - c. Select the Options menu, then Groups, then “Import security settings for this group”
 - d. In the Open dialog, browse to the C:\Public\TheLock\Settings folder
 - e. Select _DEVELOPMENT.tlg, then click Open.
 - f. The _DEVELOPMENT group is now configured.
- 41) We will now configure Group security for the _MANAGEMENT group
- a. Our _MANAGEMENT group has default “Corporate restrictions” settings.
 - b. Right click _MANAGEMENT, select “Set Default Group Security”
 - c. Check the “This group has Corporate restrictions” option, then click OK
 - d. There are just a few extra security items we will be setting
 - i. Select the Policy tab, then expand “Explorer Policy” branch, and check the option “Disable Control Panel”
 - ii. Expand the “System Policy” branch, and check the option “Disable Date/Time changes”
 - iii. Select the “File System” tab, and on the “File and Folder Security” sub-tab
 - 1. Click Add, then click the Drives button. Check mark the Removable, then check mark “No Access”
 - e. The _MANAGEMENT security group is now configured. Select the group name (if it is not already), select the “Options” menu, then “Groups”, then “Export security settings from this group”
 - f. If the Save As dialog is not already pointing to C:\Public\TheLock\Settings, browse there, then click the Save button. The file name will default to the group name. With this group’s settings saved, we will be able to re-use them when configuring the other Security Zones.

- 42) We will now configure Group security for the `_NETWORKING` group
- This group will have the same security settings as the `_DEVELOPMENT` group, with the exception of not being able to access the `C:\Dev` folder on any system they are logged into.
 - Highlight `_NETWORKING` group
 - Select the Options menu, then Groups, then “Import security settings for this group”
 - Select `_DEVELOPMENT.tlg`, then click Open.
 - We will now add the restriction for the Development folder.
 - Add the `C:\Dev` folder as restricted by selecting the File System tab
 - On the File and Folder Security sub-tab, click the Add button.
 - Add the entry for the folder name as `C:\Dev`
 - Put a mark in the No Access check box
 - The `_NETWORKING` security group is now configured. Select the group name (if it is not already), select the “Options” menu, then “Groups”, then “Export security settings from this group”
 - If the Save As dialog is not already pointing to `C:\Public\TheLock\Settings`, browse there, then click the Save button. The file name will default to the group name. With this group’s settings saved, we will be able to re-use them when configuring the other Security Zones.

- 43) We will now configure Group security for the `_PUBLIC_ACCESS` group
- Highlight the `_PUBLIC_ACCESS` group, right click and select “Set Default Group Security”
 - On the Group Utility dialog, select the option “This group has Public restrictions”, then click OK.
 - Since we are going to be using this system to only allow access to the internet, we will make the following changes:
 - Select the Policy tab, expand the “Internet Policy” branch
 - Uncheck the option “Disable Internet Explorer”
 - Uncheck the option “Disable Internet Access”
 - Expand the “Logging Policy” branch
 - Check mark the item “Enable URL Audit Logging”
 - Expand the “Violation Policy” branch
 - Check mark the item “Enable security violation account logout”
 - Select the Programs tab, then the “Secure Program Manager” sub-tab.
 - Click Add, then enter the following:
 - Program Name: Internet Explorer
 - Program executable name: `C:\Program Files\Internet Explorer\iexplore.exe`
 - Click the OK button.
 - Press the Configure button to set the preferred display settings for the Secure Program Manager. For this configuration, my window will show as:



- The `_PUBLIC_ACCESS` security group is now configured. Select the group name (if it is not already), select the “Options” menu, then “Groups”, then “Export security settings from this group”
 - If the Save As dialog is not already pointing to `C:\Public\TheLock\Settings`, browse there, then click the Save button. The file name will default to the group name. With this group’s settings saved, we will be able to re-use them when configuring the other Security Zones.
- 44) We will now configure Group security for the `_QA` group.
- Since we have already configured security for the `_QA` group, it is already set. Otherwise, we would simply use our saved `_QA` group settings by following this procedure:
 - Highlight the `_QA` group
 - Select the Options menu, then Groups, then “Import security settings for this group”
 - In the Open dialog, browse to the `C:\Public\TheLock\Settings` folder
 - Select `_QA.tlg`, then click Open.
 - The `_QA` group is now configured.

- 40) Zone 31 is now configured. Select the File menu, then Exit
- 41) You may be prompted to query users from an AD server, select No.
- 42) You will be prompted that "Settings have been changed, save new settings?", select Yes.
- 43) You will be prompted to "Add the updated settings to the Zone 31 cloned image?", select Yes.
- 44) Security Zone 31 is now configured and added to the "SMS Security Zone and Cloned Image Manager"

Creating Zone 32 for all Windows 98 systems logging into the CCTR5 NDS tree and the TEST domain.

Zone notes: This configuration is exactly the same configuration that is used by Zone 30, with the addition of the security group _TRAINING. The password authentication, and Network Group Synchronization are both set to a Netware Server.

- 1) On the SMS Security Zone and Cloned Image Manager, select Zone 30
- 2) From the menu, select SMS then “Duplicate selected SMS Security Zone”
- 3) Type a new security zone called 32, click OK.
- 4) On the SMS Security Zone Configuration dialog, set:
 - 5) The local image path to: C:\Public\TheLock\Images\Zone32\
 - 6) Set the UNC path to <\\VPCWS2003\Public\TheLock\Images\Zone32>
 - 7) Set the Description to “Windows 98 Systems with Netware on the TEST domain”
- 8) Click OK
- 9) A dialog will appear asking to configure settings for the new security zone. Click Yes
- 10) Click the System Configuration tab
- 11) Expand the Passwords branch
- 12) Enable the option “Use Netware password”
- 13) You may be prompted that the Netware client was not found on the machine. This message is OK.
- 14) Expand the Settings branch
- 15) Expand the Network Branch
- 16) Select the “Enable Network Group Synchronization” option
- 17) Change the “Users in this group are read from the group list on” drop down to “a Netware Server”
- 18) Next, Expand the Manage branch
- 19) Select Enable Security manager
- 20) Ensure the Zone entry is set to 32
- 21) Click the User Configuration tab, at the top of the Configuration Utility
- 22) This configuration we imported is from the standard Windows 98/ME configuration (Zone 30), but we will also need to add a security setting for the _TRAINING group, as they are the users who will be access these systems.
- 23) Select the “System: VPCWS2003” entry (the first entry in the user list), right click and select New Group.
 - a) In the Group Utility dialog, set the group name to _TRAINING
 - b) Check mark the option “This group has Classroom restrictions”
 - c) Uncheck the option “Add as Windows Server 2003 group on this computer”
 - d) Click OK
 - e) The _TRAINING security group is now configured. Select the group name (if it is not already), select the “Options” menu, then “Groups”, then “Export security settings from this group”
 - f) If the Save As dialog is not already pointing to C:\Public\TheLock\Settings, browse there, then click the Save button. The file name will default to the group name. With this group’s settings saved, we will be able to re-use them when configuring the other Security Zones.
- 24) Zone 32 is now configured. Select the File menu, then Exit
- 25) You may be prompted to query users from an AD server, select No.
- 26) You will be prompted that “Settings have been changed, save new settings?”, select Yes.
- 27) You will be prompted to “Add the updated settings to the Zone 32 cloned image?”, select Yes.
- 28) Security Zone 32 is now configured and added to the “SMS Security Zone and Cloned Image Manager”

Creating Zone 33 for all Windows 2000/XP systems logging into the CCTR5 NDS tree and the TEST domain.

Zone notes: This configuration is exactly the same configuration that is used by Zone 32, with the user authenticator set to a Netware server. Novell has Windows Vista drivers, but functionality is not supported under this configuration by CrashCourse Software.

- 1) On the SMS Security Zone and Cloned Image Manager, select Zone 31
- 2) From the menu, select SMS then “Duplicate selected SMS Security Zone”
- 3) Type a new security zone called 33, click OK.
- 4) On the SMS Security Zone Configuration dialog, set:
- 5) The local image path to: C:\Public\TheLock\Images\Zone33\
- 6) Set the UNC path to <\\VPCWS2003\Public\TheLock\Images\Zone33>
- 7) Set the Description to “Windows 2000 Systems with Netware on the TEST domain”
- 8) Click OK
- 9) A dialog will appear asking to configure settings for the new security zone. Click Yes
- 10) Click the System Configuration tab
- 11) Expand the Passwords branch
- 12) Enable the option “Use Netware password”
- 13) You may be prompted that the Netware client was not found on the machine. This message is OK.
- 14) Expand the Settings branch
- 15) Expand the Network Branch
- 16) Select the “Enable Network Group Synchronization” option
- 17) Change the “Users in this group are read from the group list on” drop down to “a Netware Server”
- 18) Next, Expand the Logging branch
- 19) Ensure there are no Check marks for the options “Include Security Event Log entries” and “Local audit policy”
- 20) Next, Expand the Manage branch
- 21) Select Enable Security manager
- 22) Ensure the Zone entry is set to 33
- 23) Zone 33 is now configured. Select the File menu, then Exit
- 24) You may be prompted to query users from an AD server, select No.
- 25) You will be prompted that “Settings have been changed, save new settings?”, select Yes.
- 26) You will be prompted to “Add the updated settings to the Zone 33 cloned image?”, select Yes.
- 27) Security Zone 33 is now configured and added to the “SMS Security Zone and Cloned Image Manager”

Creating Zone 34 for all Windows 98 systems logging in locally, but with networking enabled.

Zone notes: This configuration is exactly the same configuration that is used by Zone 30, with a few exceptions. First, this zone does not log into any network server, so the password authenticator will be reset, and the network group synchronization will be unchecked. Since there is not network to retrieve users, this configuration will also require that users be added to each group that is configured.

- 1) On the SMS Security Zone and Cloned Image Manager, select Zone 30
- 2) From the menu, select SMS then “Duplicate selected SMS Security Zone”
- 3) Type a new security zone called 34, click OK.
- 4) On the SMS Security Zone Configuration dialog, set:
- 5) The local image path to: C:\Public\TheLock\Images\Zone34\
- 6) Set the UNC path to <\\VPCWS2003\Public\TheLock\Images\Zone34\>
- 7) Set the Description to “Windows 98 Systems Local Access”
- 8) Click OK
- 9) A dialog will appear asking to configure settings for the new security zone. Click Yes
- 10) Click the System Configuration tab
- 11) Expand the Passwords branch
- 12) Enable the option “Use Local Windows password”
- 13) Expand the Settings branch
- 14) Expand the Network Branch
- 15) Select the “Enable settings update on startup” option
- 16) Select the “Enable Network Group Synchronization” option, and un-check it.
- 17) Expand the Manage branch
- 18) Select “Enable Security Manager”
- 19) Ensure the Zone is set to 34
- 20) We will now configure users for this Zone. Click the User Configuration tab.
- 21) Select the File menu, then “Uses and Groups” then “Network Server”
- 22) In the Lock User and Group Utility, set the server to query, then press the Query button.
- 23) Right click on the computer name at the top of the list tree, and select Uncheck all.



- 24) Place a check mark next to _DEVELOPMENT and _QA, then press Import.
- 25) The users for the groups in this Zone have now been added.
- 28) Zone 34 is now configured. Select the File menu, then Exit
- 29) You will be prompted that “Settings have been changed, save new settings?”, select Yes.
- 30) You will be prompted to “Add the updated settings to the Zone 34 cloned image?”, select Yes.
- 31) Security Zone 34 is now configured and added to the “SMS Security Zone and Cloned Image Manager”

Creating Zone 35 for all Windows 2000/XP/Vista systems logging in locally instead of into a domain.

Zone notes: This configuration is exactly the same configuration that is used by Zone 31, but with no Windows Domain features enabled.

- 1) On the SMS Security Zone and Cloned Image Manager, select Zone 31
- 2) From the menu, select SMS then “Duplicate selected SMS Security Zone”
- 3) Type a new security zone called 35, click OK.
- 4) On the SMS Security Zone Configuration dialog, set:
 - 5) The local image path to: C:\Public\TheLock\Images\Zone35\
 - 6) Set the UNC path to \\VPCWS2003\Public\TheLock\Images\Zone35\
 - 7) Set the Description to “Windows 2000/XP/Vista Systems Local Access”
- 8) Click OK
- 9) A dialog will appear asking to configure settings for the new security zone. Click Yes
- 10) Click the System Configuration tab
- 11) Expand the Passwords branch
- 12) Enable the option “Use Local Windows password”
- 13) Expand the Settings branch
- 14) Expand the System branch
- 15) Check the option Automatically create and modify users on Windows
- 16) Expand the Network Branch
- 17) Select the “Enable settings update on startup” option
- 18) Select the “Enable Network Group Synchronization” option, and check it.
- 19) Set the Setting specific option to “The Local Computer”
- 20) Expand the Manage branch
- 21) Select “Enable Security Manager”
- 22) Ensure the Zone is set to 35
- 23) Zone 35 is now configured. Select the File menu, then Exit
- 24) You will be prompted that “Settings have been changed, save new settings?”, select Yes.
- 25) You will be prompted to “Add the updated settings to the Zone 35 cloned image?”, select Yes.
- 26) Security Zone 35 is now configured and added to the “SMS Security Zone and Cloned Image Manager”

Creating Zone 36 for all Windows XP Home/Vista Home Premium systems logging in locally.

Zone notes: This configuration is exactly the same configuration that is used by Zone 35, except that this Zone has no Windows Login Integration, so that the workstations may use the Windows Welcome Screen and Fast User Switching.

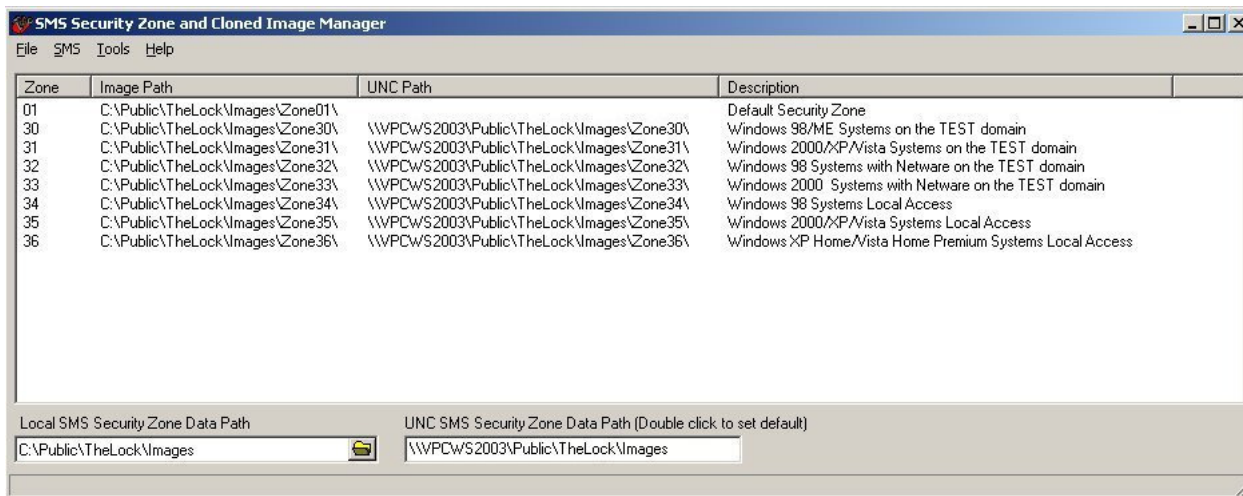
- 1) On the SMS Security Zone and Cloned Image Manager, select Zone 35
- 2) From the menu, select SMS then “Duplicate selected SMS Security Zone”
- 3) Type a new security zone called 36, click OK.
- 4) On the SMS Security Zone Configuration dialog, set:
 - 5) The local image path to: C:\Public\TheLock\Images\Zone36\
 - 6) Set the UNC path to \\VPCWS2003\Public\TheLock\Images\Zone36\
 - 7) Set the Description to “Windows XP Home/Vista Home Premium Systems Local Access”
- 8) Click OK
- 9) A dialog will appear asking to configure settings for the new security zone. Click Yes
- 10) Click the System Configuration tab
- 11) Expand the “System Startup Options” branch.
- 12) Uncheck the option “Enable Windows Login Integration”
- 13) Expand the Settings branch
- 14) Expand the Manage branch
- 15) Select “Enable Security Manager”
- 16) Ensure the Zone is set to 36
- 17) Zone 36 is now configured. Select the File menu, then Exit
- 18) You will be prompted that “Settings have been changed, save new settings?”, select Yes.
- 19) You will be prompted to “Add the updated settings to the Zone 36 cloned image?”, select Yes.
- 20) Security Zone 36 is now configured and added to the “SMS Security Zone and Cloned Image Manager”

All security Zones are now created.

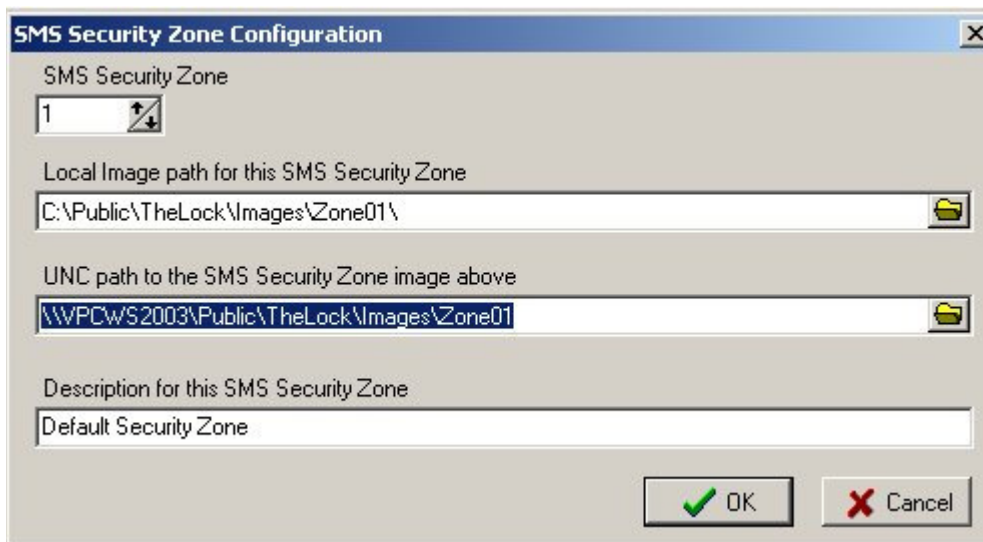
Section 6: Configuring the SMS to use the new Lock Security Zones.

The following procedure will outline the process to register each of the newly created Zones with The Lock Security Manager Server. This step is needed for the client systems to interact with the SMS server.

- 1) The SMS Security Zone and Cloned Image Manager should now look like this:

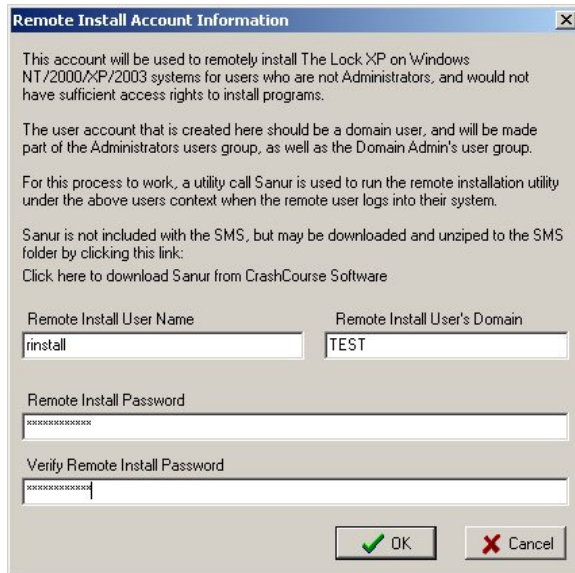


- 2) Highlight Zone 01, then from the main menu select SMS and “Edit selected SMS Security Zone”. Set the UNC path to the folder for Zone 1. In our enterprise, this path is: \\PCWS2003\Public\TheLock\Images\Zone01. The text in the edit dialog will appear as below:

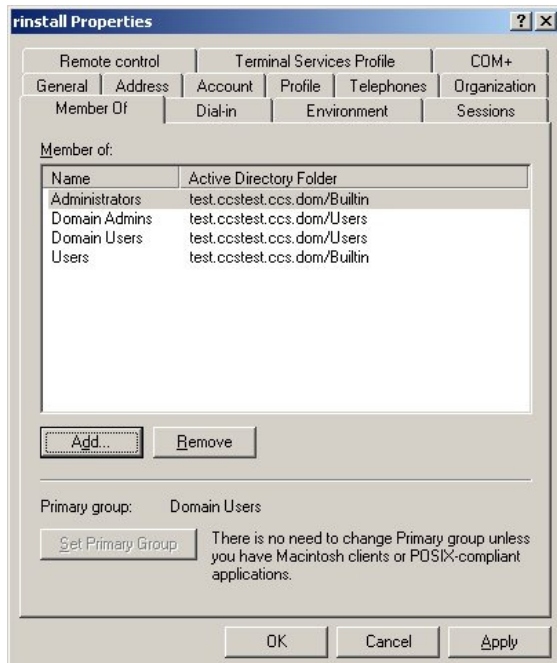


- 3) Next, we will configure the Install Account. This is a Windows account that has full administrator rights on the system, and is used to remote install The Lock on Windows NT based systems where the logged on user may not have sufficient rights to install programs. Press Select Tools, then “Configure Clone Installation Account (used for installation with Domain Login Script)”

- 4) On the Remote Install Account Information dialog, click the “Click here to download Sanur from CrashCourse Software” text. This will download the Sanur program, which is a utility used by the SMS to remotely install The Lock on Windows NT based systems. Once the file is downloaded, you will need to unzip it to the SMS installation folder. By default, this is C:\Program Files\CrashCourse\Lock2ksm. **Note:** Sanur is no longer needed by The Lock.
- 5) With the Sanur utility downloaded, enter a Remote install User Name, and password. The Domain name should have defaulted in automatically. My remote install user name is “rinstall” and the password is “passremote05”, both without the quotes.

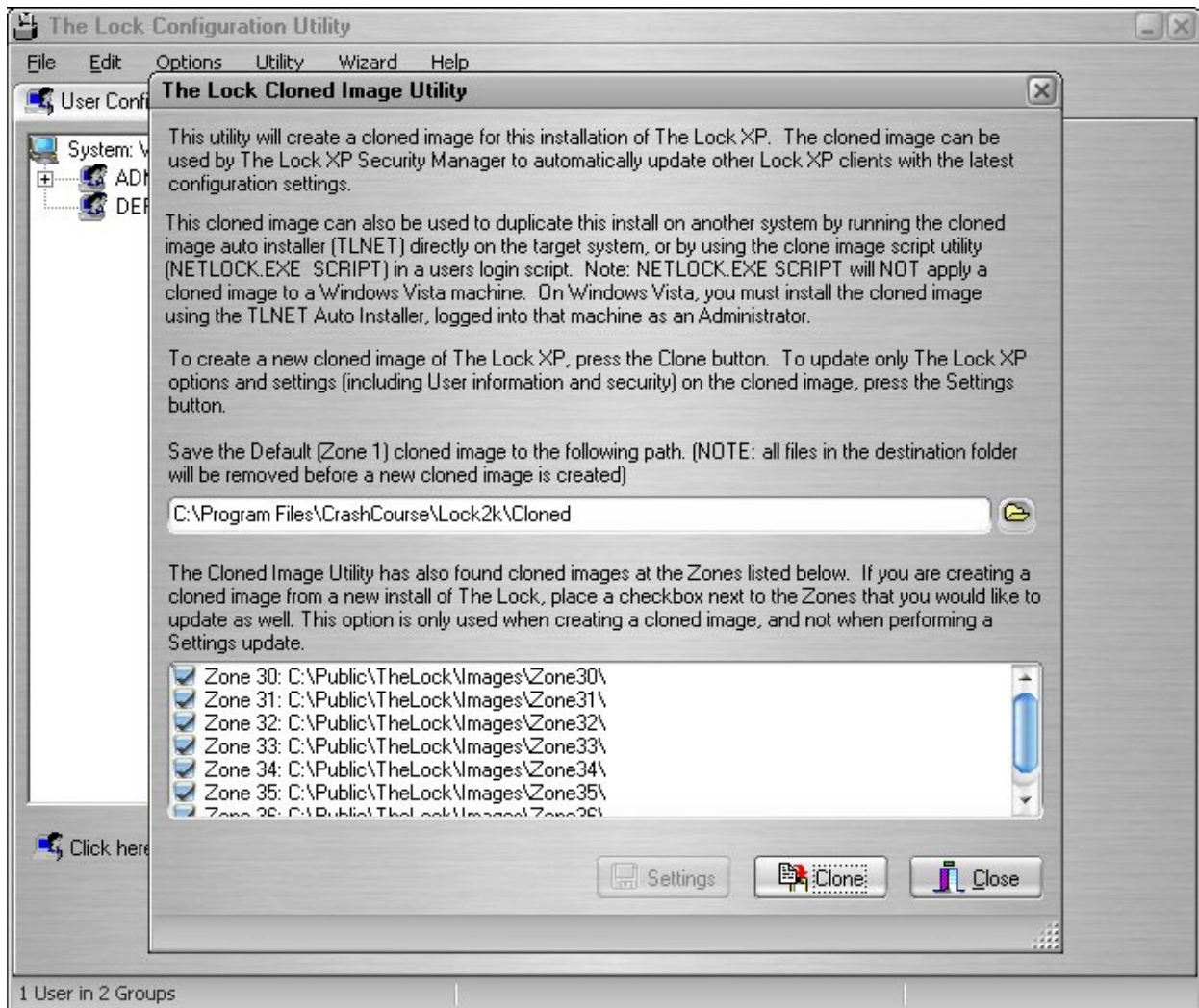


- 6) You will also need to make sure that the “rinstall” account is a member of the Domain Admins group on the local system.



- 7) Click the OK button on the “Zone Configuration and Cloned Image Manager” to continue. A prompt will appear that asks “Would you like to update your SMS user passwords with the new passwords from any added zones?” Click the Yes button.
- 8) The final step is the creation of the Cloned Images for Zones 30 to 36. Start by clicking the “Edit Zone Information” button.
- 9) On the “SMS Security Zone and Cloned Image Manager” select the tools menu item, then “Create Cloned Zone Images for all SMS Security Zones.”

10) If prompted, enter the Master Administrator password. Once The Lock Cloned Image Utility opens, you should see this:



11) Change the Default (Zone 1) cloned image path to C:\Public\TheLock\Images\Zone01\

12) Press the Clone button.

13) Press OK when prompted that The Lock will be cloned to the selected folder.

14) Once the cloned images are complete, click the OK button, then the Close button.

15) On "The Lock Configuration Utility" select File, then Exit.

16) On the "SMS Security Zone and Cloned Image Manager" select File, then Exit. Be sure to select Yes at any "Save Settings" dialogs.

Section 7: Creating auto-installers for The Lock.

The following procedure will outline the steps used to create the auto installers for Zone 1, and Zones 30 - 36.

- 1) On the SMS system, in the “SMS Configuration Utility”, select the Zones tab, if not already there.
- 2) Click Create Auto Installer.
- 3) Select the Zone you would like to export an Auto Installer for, and click OK. Our first export will be for Zone 1
- 4) Browse to the folder where the Auto Installer files will be saved. On this system, I browse to C:\Public\TheLock\Transfer, and create a new folder called “Zone01” , then click OK
- 5) Click Create Auto Installer.
- 6) Select Zone 30
- 7) Browse to the folder where the Auto Installer files will be saved. On this system, I browse to C:\Public\TheLock\Transfer, and create a new folder called “Zone30” , then click OK
- 8) Repeat the steps 5-7 above for Zones 31 – 36
- 9) Click the Close button on the SMS Configuration Utility when you are done. Be sure to select Yes at any “Save Settings” dialogs.
- 10) The Security Manager Server is now configured for multiple client connections, in multiple security zones.

Section 8: Modify Windows Logon script to install The Lock automatically upon remote logon.

The following logon script is taken directly from my PDC.

Note: CCGetOS.EXE is a free utility from CrashCourse Software that will automatically set the %username%, %computername% and %OS% on a Windows 9x/ME based system. The utility also returns an %errorcode% that is used to determine the OS type the script is running on. You may download CCGetOS.zip here:

<http://www.crashcoursesoftware.com/files/utility/ccgetos.zip>

The login script also uses the Netware environment variable NWLANGUAGE to determine if the system is logging into a Netware server. If this environment variable is detected, the script will install the proper version of The Lock.

Script "login.bat" from VPCWS2003 system.

```
@Echo Off
Echo Windows Server 2003 Logon Script
echo -----

echo Set Local Time
net time \\VPCWS2003 /set /y
echo -----

echo Map Common Public Drive to Y:
net use y: /delete
net use y: \\VPCWS2003\Public
echo.
echo -----

REM This block is used to get the OS type
if "%OS%"==" " goto OS_WIN9X
REM gets the OS type in Win_NT based systems
start /w y:\Util\CCGetOS.exe
goto OS_CHECKING

:OS_WIN9X
REM gets the OS type in Win_9x based systems
start /w y:\Util\CCGetOS.exe
call c:\setos.bat
del c:\setos.bat

:OS_CHECKING
echo User   : %username%
echo Computer: %computername%
echo OS    : %OS%
if "%errorlevel%" == "0" goto WIN_98
if "%errorlevel%" == "1" goto WIN_98
if "%errorlevel%" == "2" goto WIN_98
if "%errorlevel%" == "3" goto WIN_98
if "%errorlevel%" == "4" goto WIN_98
if "%errorlevel%" == "5" goto WIN_ME
if "%errorlevel%" == "6" goto WIN_NT
if "%errorlevel%" == "7" goto WIN_NT
if "%errorlevel%" == "8" goto WIN_2K
if "%errorlevel%" == "9" goto WIN_2K
if "%errorlevel%" == "10" goto WIN_XP
if "%errorlevel%" == "11" goto WIN_XP
if "%errorlevel%" == "12" goto WIN_WS2003
if "%errorlevel%" == "13" goto WIN_VISTA
```

```

:WIN_98
echo OS name : Windows 9x
set ZONE=ZONE32
if "%NWLLANGUAGE%"==" " set ZONE=ZONE30
goto INSTALL

:WIN_ME
echo OS name : Windows ME
set ZONE=ZONE32
if "%NWLLANGUAGE%"==" " set ZONE=ZONE30
goto INSTALL

:WIN_NT
echo OS name : Windows NT
set ZONE=ZONE33
if "%NWLLANGUAGE%"==" " set ZONE=ZONE31
goto INSTALL

:WIN_2K
echo OS name : Windows 2000
set ZONE=ZONE33
if "%NWLLANGUAGE%"==" " set ZONE=ZONE31
goto INSTALL

:WIN_XP
echo OS name : Windows XP
set ZONE=ZONE31
goto INSTALL

:WIN_WS2003
echo OS name : Windows Server 2003
goto END

REM   Notes for Vista
REM   If User Access Control is enabled, and The Lock is not yet installed on
REM   the client system, the user will be prompted with a Cancel or Allow dialog
REM   before NetLock.EXE will be allowed to complete its initial installation
:WIN_VISTA
echo OS name : Windows Vista
set ZONE=ZONE31
goto INSTALL

:INSTALL
if "%ZONE%"==" " goto ZONEERROR
Echo.
Echo Updating, please wait
y:\TheLock\Images\%ZONE%\netlock.exe SCRIPT
Echo Initial update Complete
goto END

:ZONEERROR
echo zone could not be determined

:END
echo -----

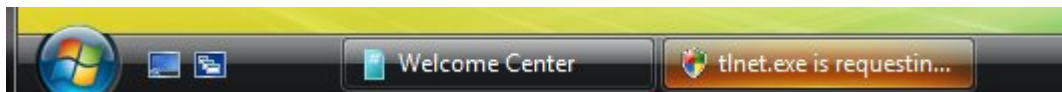
echo.

```

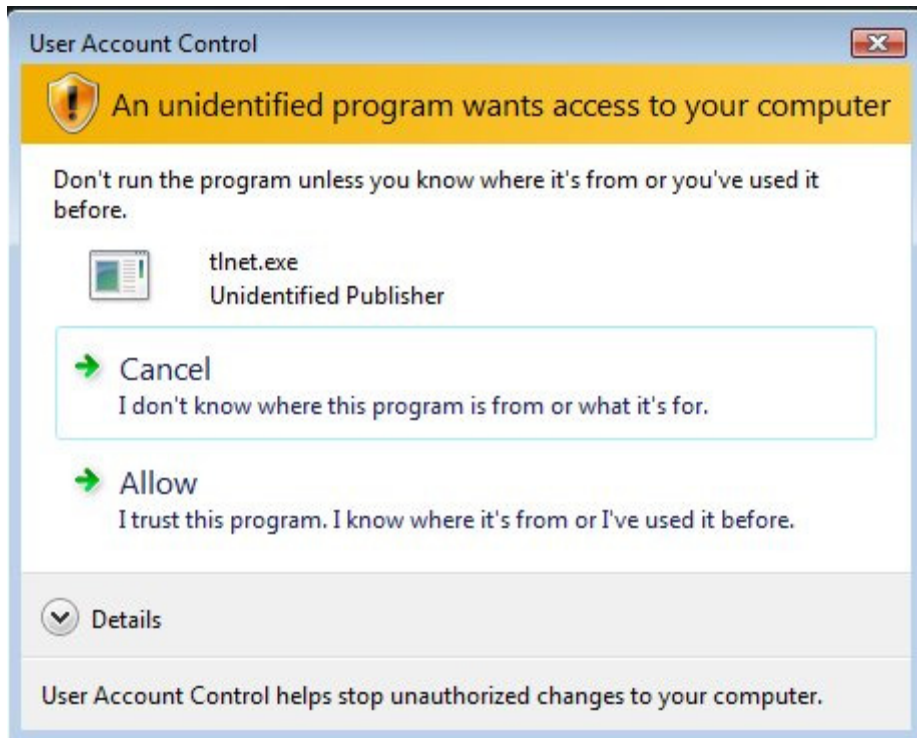
As users log into their workstations, their login scripts will run, and they will automatically have The Lock installed on their machines. Due to the usage of the RINSTALL user account, it may take more than one login into a Windows NT/2000/XP/2003/Vista system before the initial installation is completed.

Once the initial installation is complete, the users will be prompted that the system will restart. Upon restart, The Lock will be completely installed and configured on their system, according to the Security Zone they belong to. Further Lock Program and settings updates will be handled by The Lock, regardless of the configuration in the users Login Script.

On Windows Vista, If User Access Control is enabled, and The Lock is not yet installed on the client system, the user will be prompted with the following dialogs, or task bar items:



Click the “tlnet.exe is requesting” button, the following will appear:



Click Allow to start the installation. The following may appear:

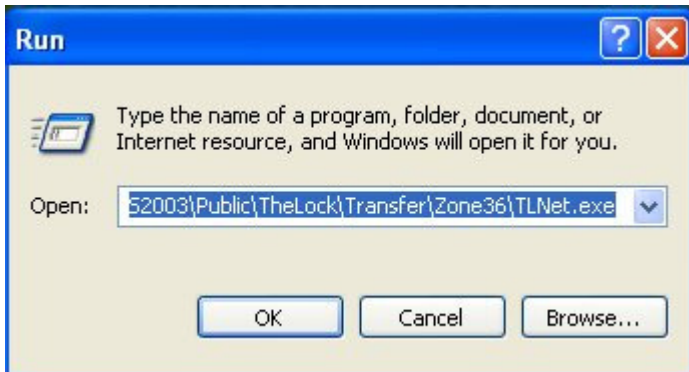


Click Unblock to continue the installation, at the end of the installation, restart the computer.

Section 9: Launch SMS Auto Installer on XP Home/Vista Home Premium, and any Windows systems not logging into the TEST domain and being installed via NETLOCK.EXE in the logon script.

For Windows XP/2000/2003 based systems

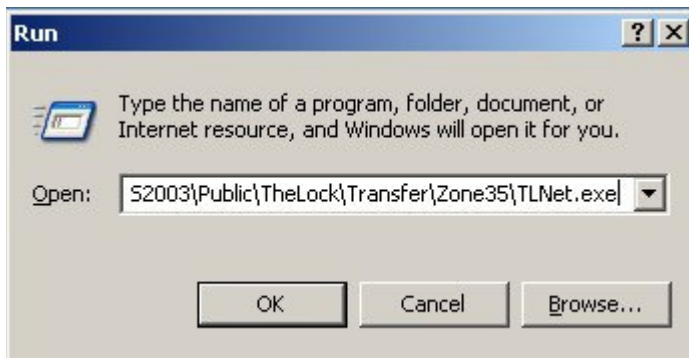
- 1) Log into Windows as a user with Administrator rights.
- 2) Click the Start Button
- 3) Select the RUN command
- 4) Browse via UNC to TLNET.EXE in the Zone36 folder on the PDC \\PCWS2003\Public\TheLock\Transfer\Zone36\TLNet.exe
- 5) The Run line will look like this:



- 6) Press OK
- 7) The Lock is now being installed on the system.

For Windows 9x/ME based systems

- 1) Log into Windows.
- 2) Click the Start Button
- 3) Select the RUN command
- 4) Browse via UNC to TLNET.EXE in the Zone35 folder on the PDC \\PCWS2003\Public\TheLock\Transfer\Zone35\TLNet.exe
- 5) The Run line will look like this:



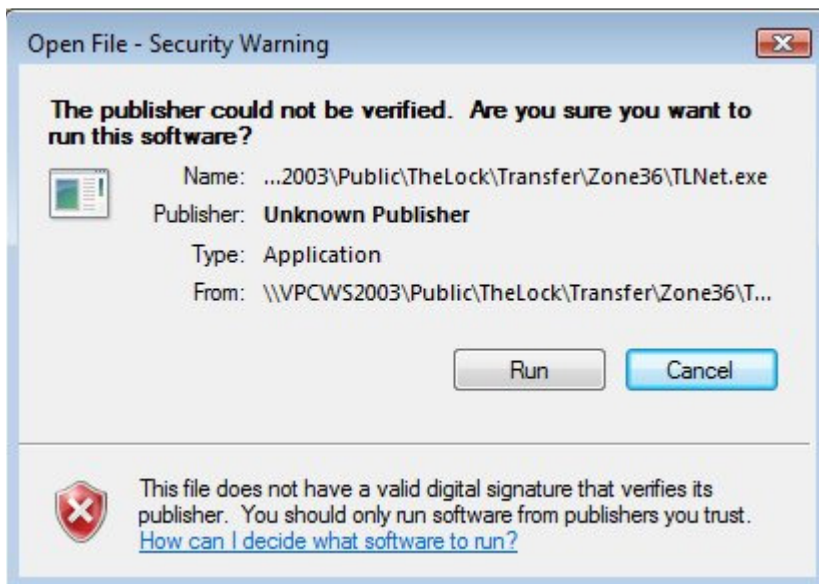
- 6) Press OK
- 7) The Lock is now being installed on the system.

For Windows Vista and later based systems

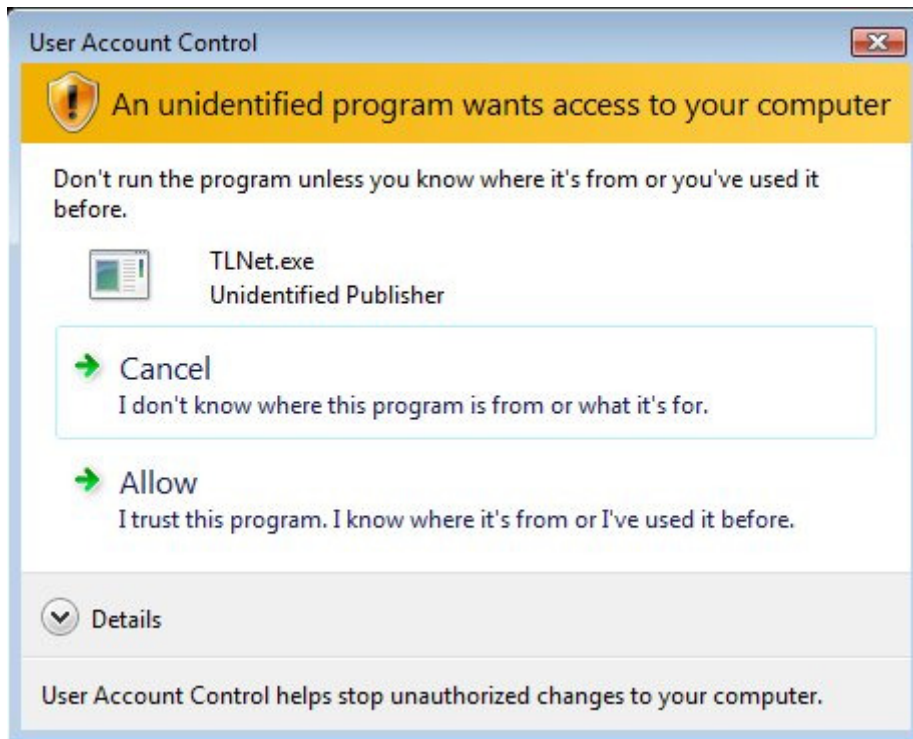
- 1) Log into Windows as a user with Administrator rights.
- 2) Click the Start Button
- 3) Select the Search Edit Box
- 4) Type the UNC path to TLNET.EXE in the Zone36 folder on the PDC
\\PCWS2003\Public\TheLock\Transfer\Zone36\TLNet.exe
- 5) The Search Box will look like this:



- 6) Press Enter
- 7) At the Open File – Security Warning, click Run.



8) When prompted by UNC, select Allow



9) The Lock is now being installed on the system. At the completion of the installation, a restart may be required.

The Lock is now completely installed, configured and administrated in an enterprise environment.