Novell

# NMAS Secure Workstation

2.1.0

www.novell.com

QUICK START

## Using Secure Workstation

### Overview

Secure Workstation will secure a workstation after a user inactivity timeout, or when an authentication device is removed. This post-login method is similar in some ways to the Workstation Access post-login method that shipped with NMAS™ 2.0. Secure Workstation is more secure than Workstation Access, and does not use a screen saver. Secure Workstation provides more features than Workstation Access.

Secure Workstation supports only Windows* 2000 and Windows XP. Workstation Access should be used on the other Windows platforms.

### Secure Workstation Post-Login Method

The Secure Workstation post-login method can be configured to provide a "lock action" on a workstation when an authentication device is removed, or when a user inactivity timeout has been reached. The possible lock actions are:

- Lock the Workstation
- Log Out of Windows
- Close All Programs
- Log Out of the Network (Client32)
- Close All Programs and Log Out of the Network

### Secure Workstation Policy

The Secure Workstation Policy can be set on the Secure Workstation object in ConsoleOne®, and in the registry of each workstation. In ConsoleOne, a separate policy can be set for each NMAS Login Sequence that employs the Secure Workstation post-login method.

When a user logs in with a sequence that includes the Secure Workstation post-login method, the Secure Workstation Service will merge the policy from the Post-Login Method with the local workstation policy. The Secure Workstation Service creates and enforces an effective policy

Novell®

using the most secure settings from each policy. The Secure Workstation Service will enforce the local policy if the Secure Workstation post-login method is not in use.

Access Control Lists (ACL) are set on the registry keys where the local workstation policy is stored. The default ACL gives Administrator and System full control, but gives users read-only access.

A GUI editor is provided for managing the local workstation policy in the registry. You can launch this editor by clicking Start > Programs > Novell > Secure Workstation > Novell Secure Workstation. Below is a summary of each of the policy settings:

- Activate Workstation Access

  The local policy will be used if this box is checked. If this box is not checked, the local policy is ignored.

- Authentication Device Removal

  If this box is checked, the lock action will be taken when an authentication device is removed.

- Inactivity Timeout

  If this box is checked, the lock action will be taken after a user inactivity timeout has been reached.

- Workstation Lock Action

  Specifies which lock action will be taken for the console user, and which lock action will be taken for Windows Terminal Services remote clients.

- Devices to Monitor for Removal

  If the Authentication Device Removal box is checked, this specifies which authentication devices will be monitored.

- Inactivity Timeout Warning

  If this box is checked, Secure Workstation will warn the user before the inactivity timeout is reached. Secure Workstation will display a dialog box with a warning. You can specify an .AVI file containing an animation to be played on the dialog, and a .WAV file containing a sound to be played. You can also specify the number of seconds that the warning should be displayed. This dialog will disappear as soon as user activity is detected.

- Force Termination of Non-Responding Programs when Logging Out of Windows

  If Log Out of the Workstation is specified as the lock action, Secure Workstation will pass the EWX_FORCE flag to ExitWindowsEx. This will speed up the logout process, but will not allow applications to save their data.

- When Closing All Programs, Forcefully Terminate Programs After *n* Seconds

When Close all Programs is specified as the lock action, Secure Workstation will post a close message to all windows of running applications. If this box is checked, Secure Workstation will forcefully terminate any applications still running after the timeout value has been reached. Applications that are forcefully terminated will not be able to save their data.

- Programs to Close

  When Close all Programs is specified as the lock action, this allows you to specify which processes should be terminated. If Close Only the Programs Specified in the Program List is checked, then only the programs specified in the program list will be terminated. Otherwise, all programs except those in the list will be terminated.

## Device Removal Detection

Device removal detection is implemented through plug-in DLLs that are registered with the Secure Workstation Service. When a user logs in to the workstation, the Secure Workstation Service starts the device removal plug-ins for the devices specified in the policy. The lock action will be taken when one of the plug-ins reports that its authentication device is no longer present.

Currently, device removal plug-ins are available for the pcProx and Universal SmartCard methods only.

## Client32

Secure Workstation can run with or without Client32™. The pcProx* and Universal SmartCard device removal plugins will also work without Client32 present.

## Secure Workstation and Workstation Access

The Secure Workstation Login Server Method (LSM) is compatible with all versions of the Workstation Access Login Client Method (LCM). If you set a Secure Workstation policy using ConsoleOne, that policy can be used when logging in with Workstation Access. The Secure Workstation LSM will determine if the client is running Workstation Access and send only the Workstation Access portions of the policy.

## Terminal Services

The Novell Secure Workstation Method supports Windows Terminal Services (WTS). In this case, a separate instance of the SMP will be launched for each WTS session. Device removal detection is not supported for WTS remote clients in this release.

## Registry Keys and Values for Secure Workstation

Key: HKLM\SOFTWARE\Novell\NMAS\<<Method Name>>\ID
(<<Method Name>> is either pcProx or Universal SmartCard)

Value: Sequence
Type: String
Data: The name of the sequence to be used when a user ID is obtained from the device. If this value exists but has no data, then the user's default sequence will be used.

Value: Tree
Type: String
Data: The tree name to be used when a user ID is obtained from the device.

Value: Server
Type: String
Data: The server to be used for login when a user ID is obtained from the device.

Key: HKLM\SOFTWARE\Novell\NMAS\<<Method Name>>\ID\LDAPServers
This key contains an ordered list of LDAP servers that will be queried for the user name when data is read from the device.