THE SECURE WORKPLACE™ for OS/2

User's Manual

Version 4.00
Manual Version June 4, 1996

Part ID: SWP40
Version:4.72
Serial: SwPs898-14120

SYNTEGRATION INC.
3811 Schaefer Avenue #J
Chino, CA 91710
U.S.A.

Tel: 1-909-464-9450
Fax: 1-909-627-3541
Compuserve ID: 73707,3331
Internet E-Mail ID: 73707.3331@compuserve.com

Table of Contents

Introduction

The Secure Workplace for OS/2 is a security and desktop management system. The product will protect your OS/2 workstation(s). from unwanted changes or intrusions. With The Secure Workplace for OS/2 you can protect, setup and support your OS/2 workstations and Desktops while reducing the support load, and therefore, the cost associated with managing one or more OS/2 Workstations.

The products Security features lets administrators grant users privileges to files, directories and workplace shell objects.These privileges include read, write, open, execute, change attributes, delete, copy, move, rename, shadow, drag, drop, visible, settings, and pop-up menu items.

Users sign-on to the workstation by entering an assigned User-ID and Password. This information can be used for single sign-on to a network or remote host.

The product includes an optional screen saver feature that will also lock the keyboard after a period of inactivity. The sign-on password is used to unlock the computer when the screen saver is invoked.

The desktop management features lets administrators provide users with different views of the same desktop or their own desktop. Administrators can assign different desktops to users, user groups, or user classes. The product integrates with Traveling Workplace, your custom program, or a Third party Desktop backup and restore product.

The Secure Workplace includes an audit trail facility. The Audit trail tracks user activities. Administrators can configure the product to record the audit information locally, and/or remotely on a file server. File server base auditing gives administrators the ability to collect audit information from multiple workstations in a network.

You can use this product in a stand alone environment or on a network

The Secure Workplace provides the following benefits:

- Prevents users from modifying the objects and files on your OS/2 workstation.
- Protects your workstation from adventurous, or malicious users. This includes inexperienced users and children.
- Enables the development of a custom desktop that can be deployed among many workstations.
- Allows you to design and deploy a custom desktop for each user or group.
- Allows you to setup a desktop you can rely on to always be the same.
- Eases the migration from a terminal based environment into a graphical user interface by allowing you to limit a user's options.
- Allows you to control the use of remote stand alone computers and notebooks.

System Setup

Setting up The Secure Workplace on your OS/2 system includes installation of the product as well as system configuration. The following information will assist you in installing the product.

The Package Contents

The Secure Workplace diskette contains the following files:

Filename	Description
SECUREWP.INF	The on-line documentation.
SCUSTWPS.INF	Customizing you OS/2 Workplace reference
SUGUIDE.INF	End User's Guide
SWOBJECT.DLL	Workplace Shell Security Class
SWOBJECT.HLP	Workplace Shell Security Class Help File
SWADMIN.EXE	Security Administration
SWADMIN.HLP	Security Administration Help File
SWMANAGE.EXE	User Sign-ON and Multi-Desktop Management
WINLISTM.EXE	The Window List Manager Program.
OBJMANAG.DLL	The Object Manager class
OBJMANAG.HLP	The Object Manager Help File
OBJEDIT.EXE	The Object Editor utility program
OBJEDIT.HLP	The Object Editor help file
PASSWORD.EXE	Password Generation program. Used by the help desk only.
SSETUP.EXE	The Secure Workplace installation program.
SHUTDOWN.EXE	The System Shutdown Program
SWUTILS.CMD	Builds Secure workplace utility objects.
SWUTILS.OMF	Object make file to create The Secure Workplace utility objects.
README.DOC	Readme file

Upgrading from a previous version

If you are upgrading from version 2.03 or lower to version 3.0 or higher you should remove the previous version before installing a higher version. Product removal can be accomplished by running the SSETUP.EXE with the /REMOVE command line option.

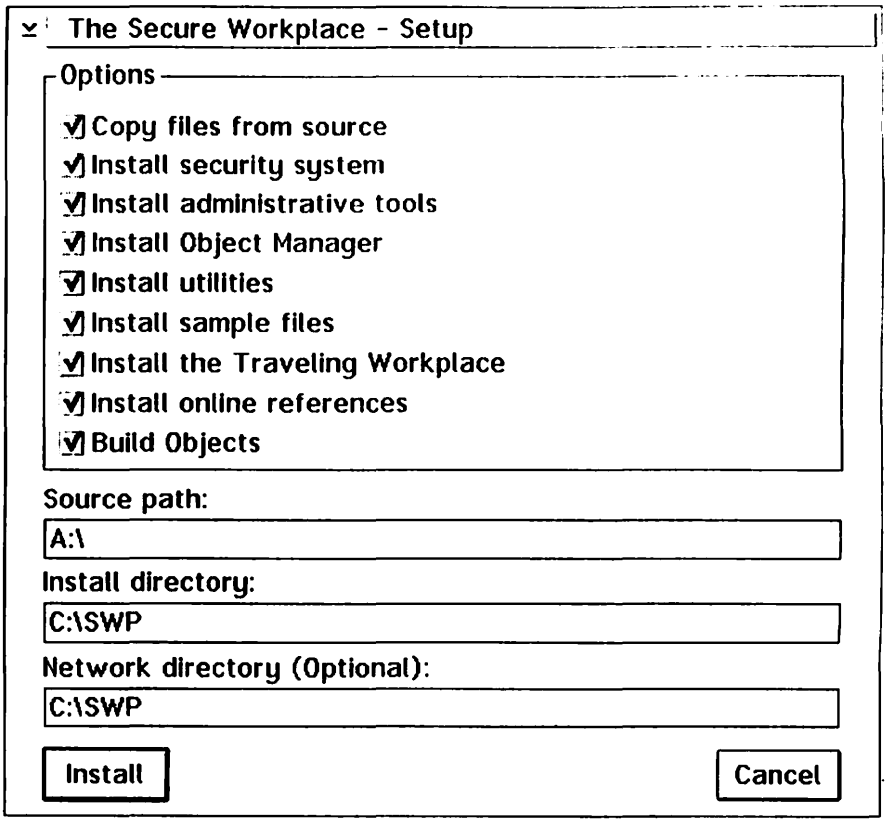
You can determine the current version by selecting the "About..." item from the desktop pop-up help menu. The Product information window will display the version number.

When you install the product over an existing version the new class DLL files are copied into a temporary directory. Your CONFIG.SYS is then modified to update the DLL files during the next system startup. You must shutdown and restart your system to complete the installation. The next time you start your system the old DLL files will be overwritten by the updated ones.

Installing The Secure Workplace

Use the SSETUP.EXE program to install The Secure Workplace. Follow the procedure given below.

1. Put The Secure Workplace diskette into a diskette drive.
2. Open a command prompt or the Drive folder that corresponds to the floppy drive containing the product diskette.
3. If you opened a command prompt, start the install program by typing *d:\SSETUP.EXE* then press enter. Where *d* is the drive letter of the floppy drive containing the diskette.
4. If you opened a floppy drive folder, open the SSETUP.EXE program. You can do this by selecting the icon and pressing enter, or by double clicking with your mouse.
5. Once the initial product information window is displayed, press the **OK** button to bring up the installation parameters window.
6. Select the installation options you require then press the install button.
7. The setup program will install the product according to the options you selected.
8. Shutdown and restart your computer to complete the installation.



In addition to updating the LIBPATH, PATH, and HELP environment variables, the setup procedure will add the following line to your CONFIG.SYS file.

SET RESTARTOBJECTS=STARTUPFOLDERSONLY

If you intend to use the Single Sign-on facility for network login we recommend that you remove the CONNECTIONS option from the AUTOSTART line in you CONFIG.SYS file. The launchpad can be a nuisance if it starts before user sign-on. We recommend that you remove the LAUNCHPAD option from the AUTOSTART line in your CONFIG.SYS file. Use the System editor or the Enhance Editor to make these changes. If you follow these recommendations then the AUTOSTART line in your CONFIG.SYS should read.

SET AUTOSTART=PROGRAMS,TASKLIST,FOLDERS

After installation and system shutdown, your "Help" cascaded menu will contain an "About..." item. Your Desktop pop-up menu will contain "Logoff..." and "Logon..." items. All objects will contain Privilege pages in their settings notebook.

When you first sign-on, the system will prompt you for a userid and password. The initial administrative User ID is "USERID" the initial password is "PASSWORD". Please remember to change this password after signing on for the first time.

You can now begin to use The Secure Workplace for OS/2 by configuring security and desktop management options in the Security Administration notebook and assigning user privileges in the object settings notebook. The **Security Administration** notebook can be found in **The Secure Workplace** folder.

The password generator and installation program are not automatically installed. These files are intended for administrative use.

Removing The Secure Workplace

Follow the procedure given below to remove the Secure Workplace product.

1. Sign on as the administrator.
2. Open the Security Administration notebook and turn to the Desktops page.
3. Turn off multiple desktop management.
4. Delete The Secure Workplace folder and the objects it contains.
5. Open an OS/2 Command Prompt.
6. Insert the product diskette into a floppy drive.
7. type **d:\SSETUP /REMOVE** then press enter. Where d is the drive letter of the floppy drive with the product diskette.
8. The program will deregister The Secure Workplace object classes and restart the Workplace Shell.
9. If The Workplace Shell was restarted but deregistration did not occur then shutdown you workstation and try the / REMOVE operation again.

10. Edit the CONFIG.SYS file with the OS/2 System Editor or the Enhanced Editor.
11. Remove all references to the The Secure Workplace install directory (usually \SWP\BIN, \SWP\DLL, \SWP\HELP).
12. Change the SET RUNWORKPLACE statement back to its original setting.
    (ie. SET RUNWORKPLACE=C:\OS2\PMSHELL.EXE)
13. Remove the TWPINI, SWPPATH, SWPNETPATH, AUTOGUEST, and GUESTNAME environment variable statements.
14. Delete the files in the \SWP installation directory.
15. Restart your workstation.

Setup command line options

When you run the System Setup program (SSETUP.EXE) from an OS/2 command prompt, a REXX script, or a CMD file you can specify start-up options. The command line syntax is:

SSETUP [options]

The available options are:

/S=SourceDir The directory that contains The Secure Workplace files. The default directory is the same as the location of the SSETUP.EXE file.

/T=TargetDir Specifies the target directory to copy the product files into. The default target directory is "C:\SWP."

/RSP=RspFile Specifies a response file to be used for unattended installation. A sample response file (SSETUP.RSP) is included on the distribution diskette. If you specify this option then the NOLOGO and NOPROMPT options are automatically set.

/L=LogFile Names the file to be used to log all operations.

/N=Station Specifies the station name to be associated with this workstation. The station name is used for all audit operations. A station name is particularly useful when you are auditing to a network drive in an environment where there is more than one workstation.

/NOLOGO Causes the setup program to bypass the initial product information window.

/NOPROMPT Causes the setup program to bypass the installation parameters and the progress log windows. This parameter is needed for unattended installation.

/REMOVE Instructs the setup program to degerister The Secure Workplace classes from the system.

The SSETUP.EXE program can be use for unattended installation and customization in a remote or network environment.

Be careful to separate each option with one or more spaces.

Administrator's Guide

Now that you have installed The Secure Workplace, your first task is administration. Administration is performed from the Security Administration notebook and from the Privileges Tab in every objects Settings notebook. All options have safe defaults. You only need to concern yourself with the items you will use. This chapter is divided into the following sections:

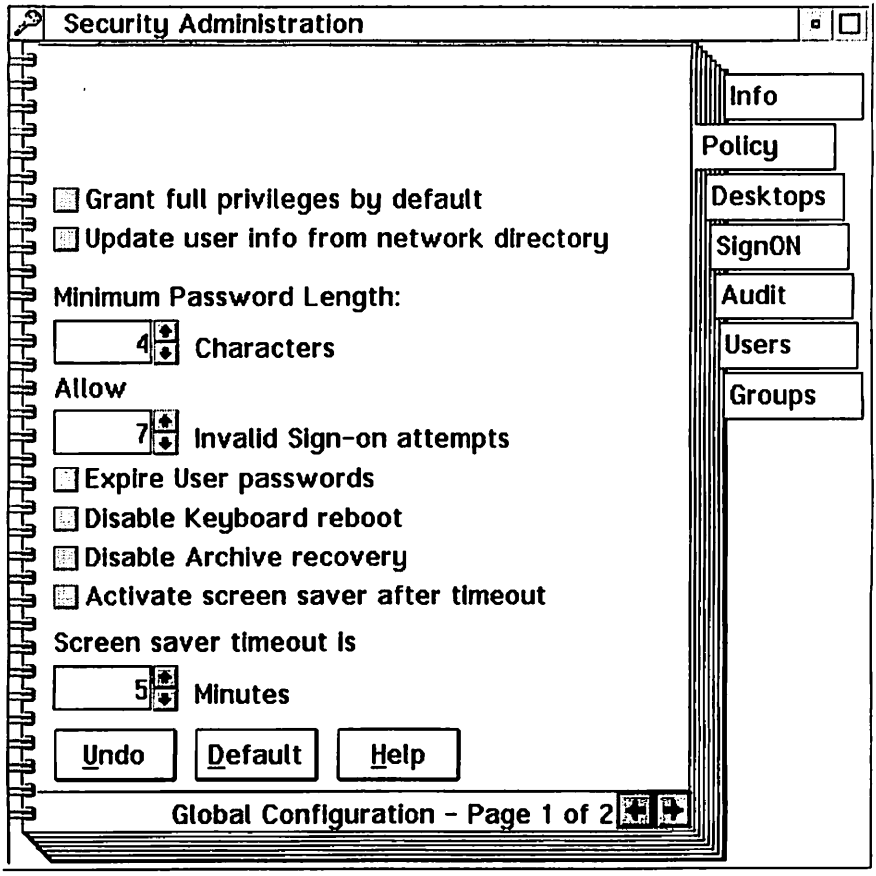
1. Signing on the first time.
1. Security Policy.
2. Dynamic Passwords.
3. User and Single Sign-ON.
4. Audit system Events.
5. Defining Users .
6. Defining User Groups.
7. Granting User Privileges.
8. Desktop Management

Signing on for the first time

When you turn on your computer the system will prompt you for a userid and password. The initial administrative User ID is "USERID" the initial password is "PASSWORD". Please remember to change this password after signing on for the first time. If the Sign-ON window does not appear, bring up the desktop pop-up menu and select the "**Logon...**" option. The Secure Workplace folder contains two special objects you can move to the Desktop. These are titled **Sign-ON** and **Sign-OFF.** Double click on the Sign-ON object to log-on. Double on the Sign-OFF object to log-off.

Security Policy

In the Security Administration notebook use the Policy page to specify your System Security Policy. If you purchased an Enterprise license then all items on this page can also be configured by running the setup program with a response file.



The Policy items are as follows:

Grant public privileges by default
When you check this box The user will be granted full privileges to any Workplace Object, File, or Directory that does not have an access control definition. This has the effect of making items without privileges public. When you leave this box unchecked, items without privileges will automatically be protected.

Update User info from Network directory
When you check this box The Secure Workplace will update Users, Groups, and Privileges from a data file in The network directory. This update occurs just after a user signs on to the workstation. With this feature you do not have to add users and privileges to each workstation manually. Just copy the Security

Profile (SECUREWP.INI) to the network directory. You can configure this feature with any edition of the product, but it is only implemented when you purchase an Enterprise license.

Minimum Password Length
This spin button allows you to set the minimum password length allowed. This policy is enforced when users attempt to change their password. Existing passwords are not affected.

Invalid Sign-on attempts
This field sets the allowed number of invalid sign-on attempts. When the specified number of illegal sign-on attempts are reached the system will lock until an administrator signs-on. You can disable this feature by setting the value to zero.

Expire User Passwords
Check this box to force users to change their passwords after a specified number of logins. The number of allowed sign-ons are specified in each user's definition. See Page 1 in the User Tab. This feature is enforced when you use local authentication.

Disable Keyboard reboot
Check this box to disable the use of the <CTRL+ALT+DEL> key combination.

Disable Archive Recovery
Check this box to prevent users from restoring desktops with <ALT+F1> at system startup.

Activate screen saver after timeout
Check this box to activate the screen saver after the workstation has been inactive for the specified number of minutes. The unlock password automatically changes to the user's sign-on password. This unlock password is encrypted and stored in dynamic memory (RAM). You can be assured that it is safe from prying eyes. All other aspects of the screen saver are configurable from the Lockup Tab in the Desktop settings notebook. Administrators can always unlock the workstation with a dynamic password. The screen saver feature will become active after you reboot your computer.

Screen Saver timeout
Sets the number of minutes of inactivity you want to allow

before the system locks the keyboard and mouse.

Dynamic Passwords

Dynamic Passwords are our software implementation of ID Card technology. These passwords are are based on the system time, the system date, and a Seed string that you specify. With this implementation you can define a dynamic password that is unique to your organization, department, or network domain.

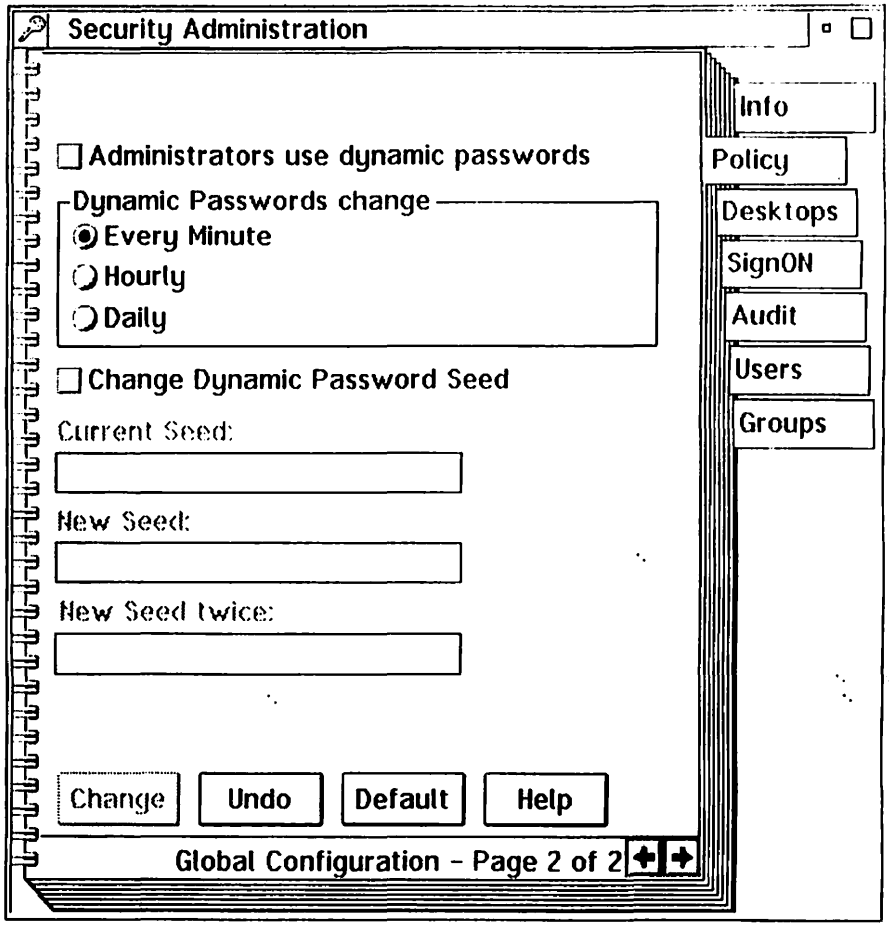
Administrators can be required to enter a dynamic password to obtain administrative privileges on a workstation. Since the password is valid for a short period of time, it doesn't matter if users look on when an Administrative password is being entered at the sign-on window.

Dynamic passwords can be particularly handy when you are administering off-site workstations. With this feature, you can give users one time access to perform administrative functions without fear that they will be able to use the same password again.

A companion password generator program (PASSWORD.EXE) runs on a separate machine. Perhaps at a help desk or in the administrator's office. You enter the date, time, and period and the password generator gives you the dynamic password for the date, time, and period you specified.

Each workstation can be configured to use a different Dynamic password seed. By default, the initial seed value is "PASSWORD". The seed value can be set in the security administration notebook or during setup when you use a response file. You should make sure that the machine running the password generator program has the same seed string as the machine whose password you wish to discover.

Dynamic passwords are configured in the Security Administration notebook on page 2 of the **Policy** tab. If you purchased an Enterprise license then all items on this page can also be configured by running the setup program (SSETUP.EXE) with a response file.



Administrators use Dynamic Passwords
Check this box to require administrators to use dynamic passwords for local authentication.

Dynamic Passwords change
Select one of the buttons to configure the dynamic password period. Dynamic passwords can be configured to change every minute, every hour, or every day.

Change Dynamic Password Seed
Check this box to allow changes to the seed string.

To change the seed, open the Security Administration notebook and turn to page 2 of the Policy Tab. Type the current seed into the entry field, then type the new seed into each of the respective new

seed fields. Press the "Change" pushbutton once the fields are filled in.

Special Note In the Standard and Evaluation editions, Dynamic passwords are based only on the system clock. Enter the password as YYYYMMDDHHmm where YYYY is the year, MM is the month, DD is the day, HH is the hour, and mm is the minute. These system clock values are displayed in the sign-on window for your convenience. Dynamic passwords are not particularly secure in these editions.

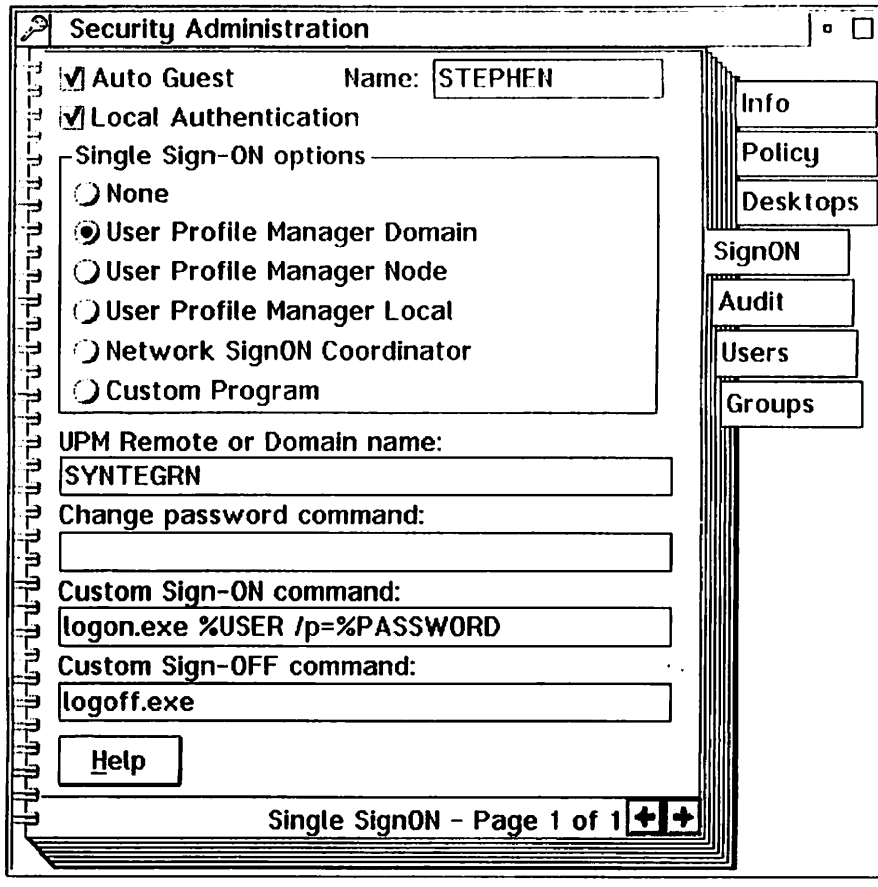
User Sign-ON

Configure user Sign-ON operations in the Signon page of the Security Administration notebook. If you purchased an Enterprise license then all items on this page can also be configured by running the setup program (SSETUP.EXE) with a response file.

At start-up The Secure Workplace for OS/2 displays a sign-on window that prompts the user for an identification name and a password. The product also provides Single Sign-On to any network operating system or remote host. With this feature you can configure the system such that users need only identify and authenticate once.

If you use Single Sign-ON and you have a network requester installed, then you should consider updating the AUTOSTART parameter in your CONFIG.SYS File. The AUTOSTART CONNECTIONS options will sometimes cause a network logon window to appear at system startup. By removing the CONNECTIONS option you can prevent this from occurring.

The logon procedure is executed after the User ID and password are entered. You can configure a logon environment using existing programs such as your network operating system's login program or customize the environment by creating your own scripts.



Auto Guest

When you choose this option the system will automatically authenticate the Guest User and bypass the sign-on window. The Guest user is defined in the CONFIG.SYS by assigning the GUESTNAME environment variable. The Guest User has no privileges unless you assign them.

Guest Name

Specify the Auto Guest ID in the **Name** entry field. This field is used to create the GUESTNAME environment variable. For the auto guest feature to work properly, the guest name and the guest password must be the same.

Local Authentication

When you choose this option the system allows users to decide whether to sign on to the local workstation. A corresponding

local sign on checkbox will be available in the login window. If you use the workstation in a stand-alone mode, local authentication must be allowed.

Single Sign-ON Options

Select one of the Single Sign-ON options described below. When you choose an option other than none, The system allows the selected login procedure to authenticate the user. Single signon in a network environment provides the advantage of allowing you to manage passwords in one place - on the server.

None

The None option implies that the Security System will not execute any external user authentication procedure. If this option is selected the system defaults to local authentication.

User Profile Manager Domain

The User Profile Manager (UPM) Domain option is appropriate when you have a IBM LANServer or IBM WARPServer network. To use this option you must first install the IBM Network Requester.

User Profile Manager Node

The User Profile Manager Domain option is appropriate when you have an IBM DB2 Server on a network. To use this option you must first install the necessary IBM products.

User Profile Manager Local

The User Profile Manager (UPM) Local option is appropriate when you have IBM WARP CONNECT, DB2, LANSERVER, WARPSERVER, TCP/IP, COMMUNICATIONS MANAGER/2, or any other IBM product that installs UPM on your local workstation.

Network SignON Coordinator

Choose this option to sign-on using IBM Network SignON Coordinator (NSC). NSC can be used for logins to Novell Netware, IBM LANServer, IBM WARP Server, and an APPC Host. You must first configure the NSC.INI file and test it before commiting to this option.

Custom Program

Choose this option to execute a background authentication

program. You pass the USERID and PASSWORD entered by the user to this authentication program. The program should return an exit code of zero to signal that the user is correctly authenticated. If you need to use third party authentication programs or custom in-house programs for sign-on and authentication then this is your option of choice. UPM and NSC can also be invoked with this option.

UPM Remote or domain name
Enter a field that specifies the UPM remote or Domain. This field is required for UPM node logon and can be used during UPM Domain logon. The user will also have an opportunity to change this value at sign-on time.

Change Password command
This command is used to change user passwords when you choose a custom program for Single Sign-on.

Custom Sign-ON command
This command is executed when you have selected the Custom Single Sign-On option and after the user and password are entered. Successful completion is indicated by an exit code of zero. You should specify the %USER and the %PASSWORD keywords to pass the user name and password to the custom program.

Custom Sign-OFF command
This command is executed to perform a user logoff. Enter your logoff program in the field.

Notes:

The Secure Workplace for OS/2 invokes User Profile Manager directly when you choose one of the UPM options. To enable any of these options, you must first install an IBM product that contains UPM. Make sure that the UPM32.DLL file is available and in the LIBPATH.

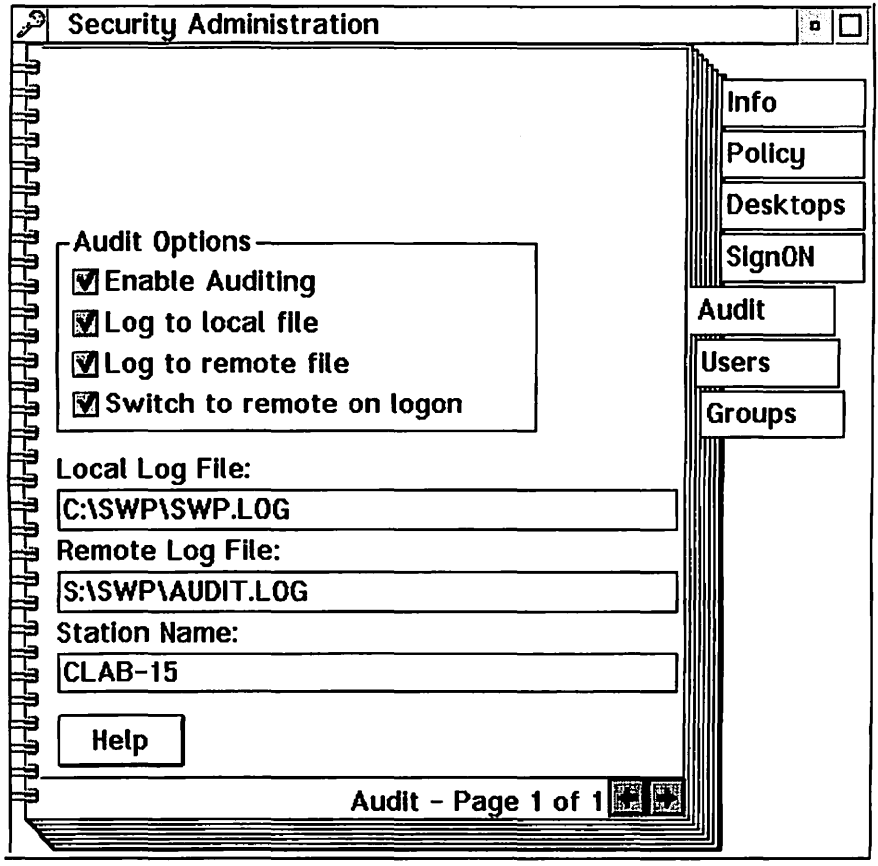
The Secure Workplace for OS/2 invokes Network Signon coordinator directly when you choose the NSC option. To enable

this feature you must first install and configure NSC. Make sure that the NSCAPI.DLL file is available and in the LIBPATH.

Refer to the section titled **Specifying commands** for detailed information on how to enter commands.

Auditing System Events

The Audit page in the Security Administration notebook allows you to configure your secure workplace for audit operations. If you purchased an Enterprise license then all items on this page can also be configured by running the setup program with a response file.



The audit log records the operations that take place on you computer. The Audit log file can be located on a workstation or on

a network file server. The following parameters allow you to configure your workstation for auditing.

Enable Auditing
Specifies whether the workstation will audit events to the log file.

Log to local file
Tells the system to write all events to the local log file. This option is ignored if auditing is disabled.

Log to remote file
Tells the system to write all events to the remote log file. This option is ignored unless auditing is enabled, User logon is enabled, and user logon is verified.

Switch to remote on logon
Tells the system to write events to the remote log file when a user logon is verified.

Local Log File
Specifies the path and filename of the log file on the workstation.

Remote Log File
Specifies the path and filename of the file server log file.

Station Name

Specifies a unique name for your workstation. This name will be used by the audit facility to identify your workstation in the log file. You should configure the station name in a network environment with more than one workstation.

Notes:

The log file can be viewed with any text editor or browser. You are responsible for managing the log file. We intend to supply a log file viewer in a future version.

Audit operations occur in the background. You will not be alerted if the log file names you specify are incorrect. Check the filename carefully, then verify that the audit information is being written.

The Audit system is fault tolerant. If the audit files are invalid the

system will bypass the audit step without a perceptable delay. The audit facilty will detect errors like:

- File not found.
- Path not found.
- Invalid file name.
- Disk full.
- Invalid Drive specified
- File write protected.

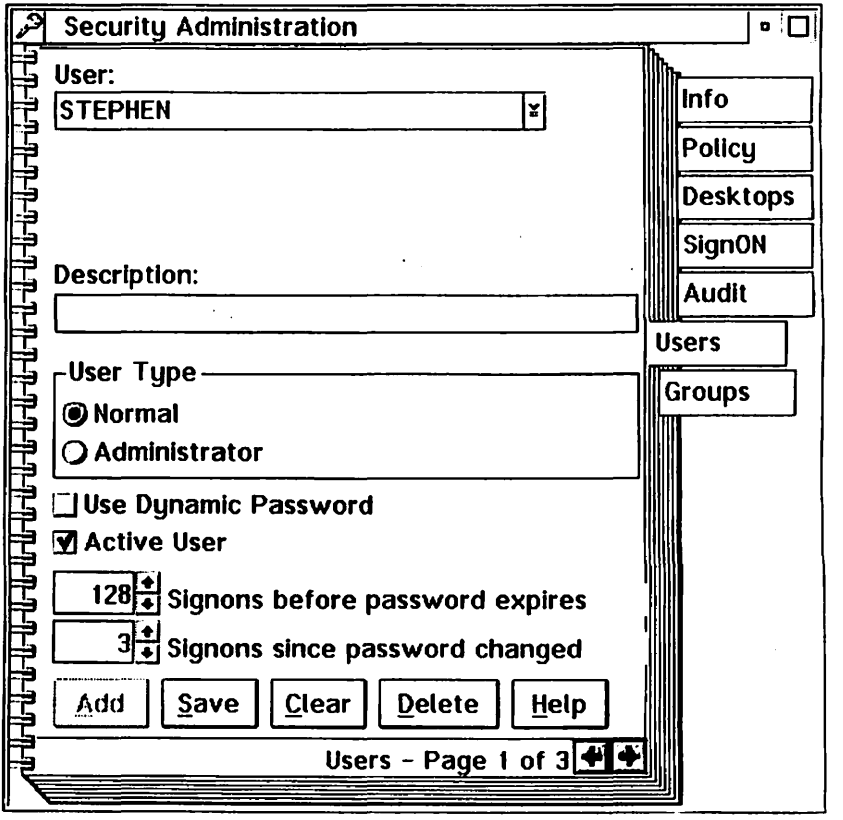
In a network environment where the remote log file is shared between multiple workstations the audit facility waits for write access. The audit system will wait 5 seconds and retry the write operation at 64 millisecond intervals during this period. After 5 seconds the system will abandon the write operation.

In earlier versions of this product, the audit facility caused system delays when the log file names were specified incorrectly. We have made every effort to detect and handle audit file problems. If you experience intermittent system delays when auditing is enabled then check the log file name. Report such behavior to our technical support staff.

Defining Users

Users are defined in the Security Administration notebook. Three pages are available in the User Tab. If you purchased an Enterprise license the user definitions can be automatically updated from the SECUREWP.INI file in the Network directory.

If you are administering OS/2 workstations in a network environment you may be particularly concerned with duplicating the user database. We suggest that you pay close attention to the **Include Everyone** option when defining **User Groups**. This option may help to minimize your work. The **Network Update** capability of the Enterprise version will also help to ease your concerns since you need only define The Secure Workplace user database in one place. We intend to supply user database export and import functions with a future version.



The user definition items are as follows.

User

Type a unique user name in this field. If you intend to use Single Sign-ON then the user name should correspond to a pre-existing name that you have defined elsewhere. You can also select users that have already been defined by pressing the drop down list button to the right of the entry field.

Description

Enter the users full name or some other description here. You can use up to 40 characters for this purpose.

User Type

Select Normal or Administrator. Normal users have there privileges set by administrators. Administrators have full privileges.

User Active

Allows you to temporarily deactivate the user without removing the definition.

Use Dynamic Password

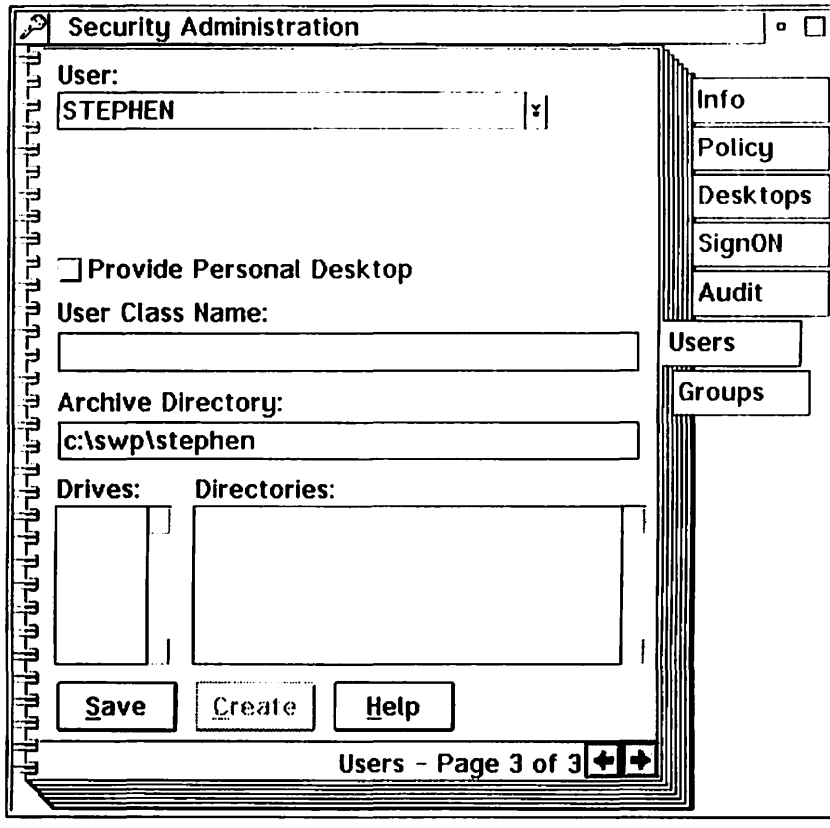
Enforces the use of a dynamic password. This feature applies to local administrators only.

Sign-ons before password expires

Select the number of times a user can sign-on before a password change is required. This value is enforced when local authentication is used.

Sign-ons since password changed

This report item keeps a count of the number of times a user has signed on since the last password change. You can reset this value to invalidate or renew a password. Changing the password resets this value.



User Class Name

Class names are defined on page three of the user tab. Enter a class name for the user. This string is used as the %CLASS substitution parameter for Multiple Desktop Management. A class name is intended as an alternate method for grouping users. Some examples of class names are STUDENT, INSTRUCT, MANAGER, TELLER, SALES, CLERK, ACCOUNTS. Class names are managed separately from User Groups, but nothing prevents you from creating user groups that exactly match the class names you define. Class names can be used to represent filenames, subdirectories, a filename prefix, a filename suffix, or any other purpose.

Archive Directory

The user's archive directory is defined on page three of the User tab. Enter an archive directory for the user. This string is used

as the %ARCHIVE substitution parameter for Multiple Desktop Management. You can assign the same directory to more than one user.

Adding a User

1. Open the Security administration notebook and turn to the Users tab.
2. Type a user name in the user field.
3. Type a user description in the description field.
4. Select a user type.
5. Make any other selections on page one.
6. Press the Add button.

Changing User information

1. Open the Security Administration notebook.
2. Turn to the User page containing the information you want to change.
3. Select a user from the drop down list.
4. Make the changes you require.
5. Press the Save button.

Deleting a User

1. Open the Security Administration notebook.
2. Turn to the Users tab page 1.
3. Select a user from the drop down list.
4. Press the Delete button.

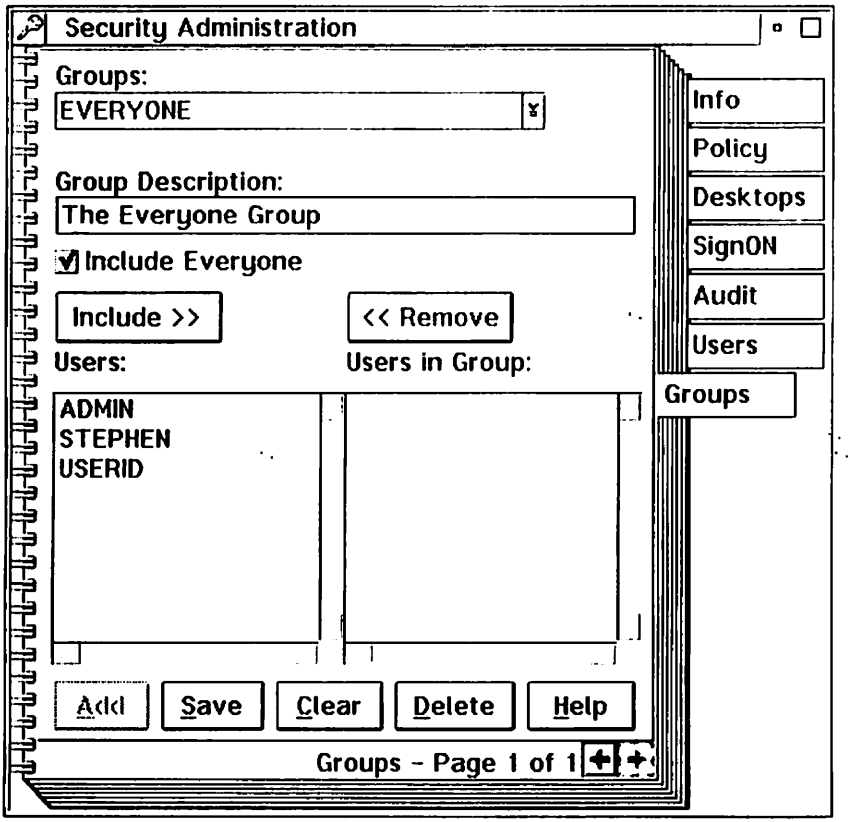
Changing a User's password

1. Open the Security Administration notebook.
2. Turn to page 2 in the User tab.
3. Select a user from the drop down list.
4. Enter the current password. The initial password is the same as the user's name.
5. Enter the new password twice.
6. Press the change button button.

Password changes can also be performed at the user sign-on window.

Defining Groups

Users Groups are defined on the Group page in the Security Administration notebook. If you purchased an Enterprise license then Group definitions can be automatically updated from the SECUREWP.INI file residing in the Network directory.



User Groups are used to reduce the labor of assigning User privileges. The Items are described in the following paragraphs.

Groups

You can enter new group name in the entry field or select from any of the existing groups in the drop down list.

Group Description

Enter any description you desire. The description can be up to 40 characters in length.

Include Everyone
Check this box to automatically include every user in the group. This also includes undefined users that are authenticated by the Single Sign-ON process. New users will automatically be included as well. Use this option to create EVERYONE groups.

Users in Group
The list of users currently in the group. This list is ignored when the Include Everyone box is checked.

Adding a Group

1. Open the Security Administration notebook and turn to Group tab.
2. Type a Group name in the Group field.
3. Enter a description in the description field.
4. Check or uncheck the Include Everyone box.
5. Select from the Users list then press the Include button.
6. Select from the Users In Group List then press the Remove button.
7. Press the Add button.

Changing a Group

1. Open the Security Administration notebook and turn to Group tab.
2. Select a Group from the list.
3. Check or uncheck the Include Everyone box.
4. Select from the Users List then press the Include Button.
5. Select from the Users In Group List then press the Remove button.
6. Press the Save button.

Deleting a Group

1. Open the Security Administration notebook and turn to Group tab.
2. Select a Group from the drop down list.
3. Press the Delete button.

Press the Clear button to cancel any operation.

Defining User Privileges

After you have installed The Secure Workplace and rebooted your computer, Privilege pages are added to every Workplace Object's settings notebook. These pages are grouped under a Privileges tab. You can use this interface to assign user or group privileges for Files, Directories, and Workplace Shell objects.

For the purpose of this discussion and your own general understanding we will refer to Files, Subdirectories, and Workplace Shell objects with the term object.

Administrators grant users or groups privileges to objects. A user or group can be granted the privilege to see, open, execute, copy, move, delete, rename, shadow, drag, drop, read, write or change attributes of an object. These and other privileges are based on Workplace Object pop-up menu items, Workplace Object styles, and File Access operations.

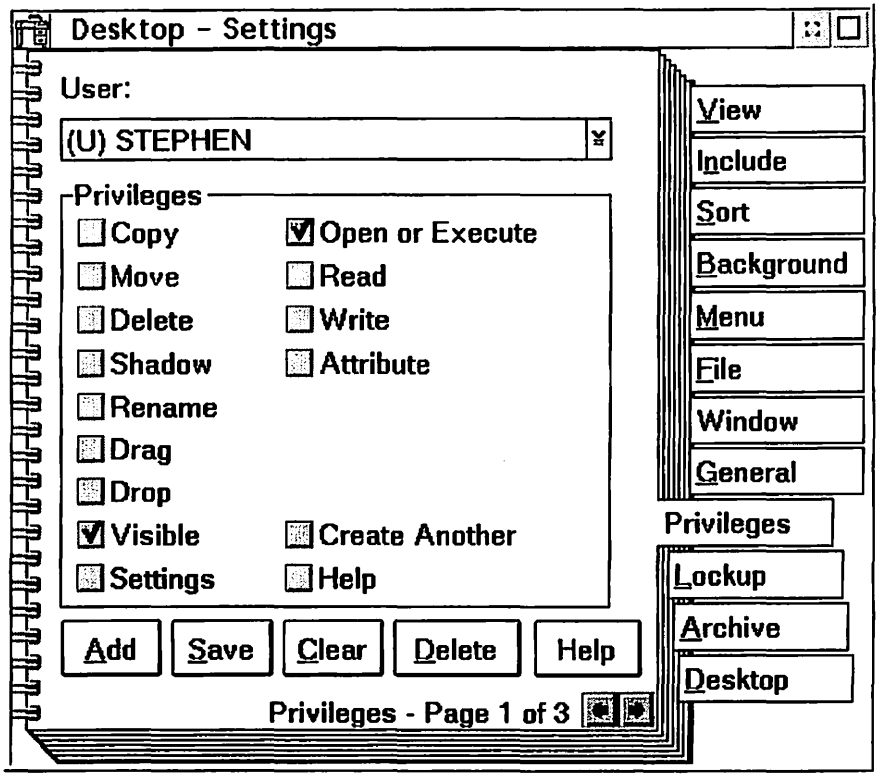
When an object has no assigned user privileges, The Secure Workplace searches up the parent chain of the directory tree to find the first parent with assigned privileges. In the case of desktop objects the search stops when the desktop is reached. In the case of objects outside the desktop the search stops when the root directory is reached. In other words, objects with no assigned user privileges inherit the privileges of a parent folder or directory. If no assigned privilege is found then the user is granted default privileges. Default privileges may be Public or Private depending on the option you choose on the Security Policy page. Administrative labor is minimized by assigning privileges to folders and directories at the highest levels of the directory tree.

To get to an object's Privilege page:

1. Move your mouse pointer over the object.
2. Press the right mouse button to bring up the pop-up menu.
3. Select the **Settings** option to open the settings notebook.
4. After the settings notebook opens, turn to the **Privileges** tab.

Basic Privileges

Use Privileges page 1 to assign basic privileges for any object.



Administrators can grant the following basic privileges:

Copy
Check this box to allow the user to copy the object from one folder to another. Uncheck this box to remove the **Copy...** item from the object's pop-up menu and enforce the NO COPY style.

Move
Check this box to allow the user to move the object between folders. Uncheck this box to remove the **Move...** item from the object's pop-up menu and enforce the NO MOVE style. If Drag is allowed the user can still relocate the object inside its folder.

Delete
Check this box to allow the user to delete the object. Uncheck this box to remove the **Delete...** item from the object's pop-up

menu and enforce the NODELETE style. With this permission removed the user cannot delete the object with a delete key or by dropping it on the shredder. The Object Manager or Object Editor can still delete Workplace objects. The file access control driver gives additional protection from command prompts and file manager programs.

Shadow
Check this box to allow the user to creates shadows of the object. Uncheck this box to remove the **Create Shadow...** item from the object's pop-up menu and enforce the NO SHADOW style.

Rename
Check this box to allow users to change the object's title. Uncheck the box to prevent the user from changing object's title or filename. Attempts to change the title through the general page in the settings notebook or by direct manipulation will fail. The file access control driver also enforces this privilege to give additional protection from command prompts and other programs.

Drag
Check this box to allow the user to drag the object. Remove the check mark to prevent the object from being dragged with the right mouse button. The Pickup menu choice will also be removed. The NODRAG style can be particularly quirky on shadow objects.

Drop
Check this box to allow the user to drop other objects onto the object. When you remove this privilege, nothing can be dropped on or into the object. This can be particularly helpful on folders.

Settings
Check this box to allow the user to open the object's settings notebook. Deny this privilege to prevent the user from changing the object's settings.

Visible
Check this box to allow the user to see the object. Deny this privilege to prevent the user from seeing the object. This is the

most basic privilege. If users cannot see the object they cannot perform any operations on it. By granting or denying visibility you can effectively give each user or user group a different view of the same desktop.

Open or Execute
Check this box to let the user open the object. Deny this privilege to prevent the user opening the object. This is the second basic privilege. This permission is also enforced at the operating system level by the file access control driver supplied with the professional edition.

Read
Check this box to let the user open the file for read access. Deny this privilege to prevent the user from reading the file. This permission is enforced by the file access control driver supplied with the professional edition.

Write
Check this box to let the user open the file for write access. Deny this privilege to prevent the user from writing to the file. This permission is enforced by the file access control driver supplied with the professional edition.

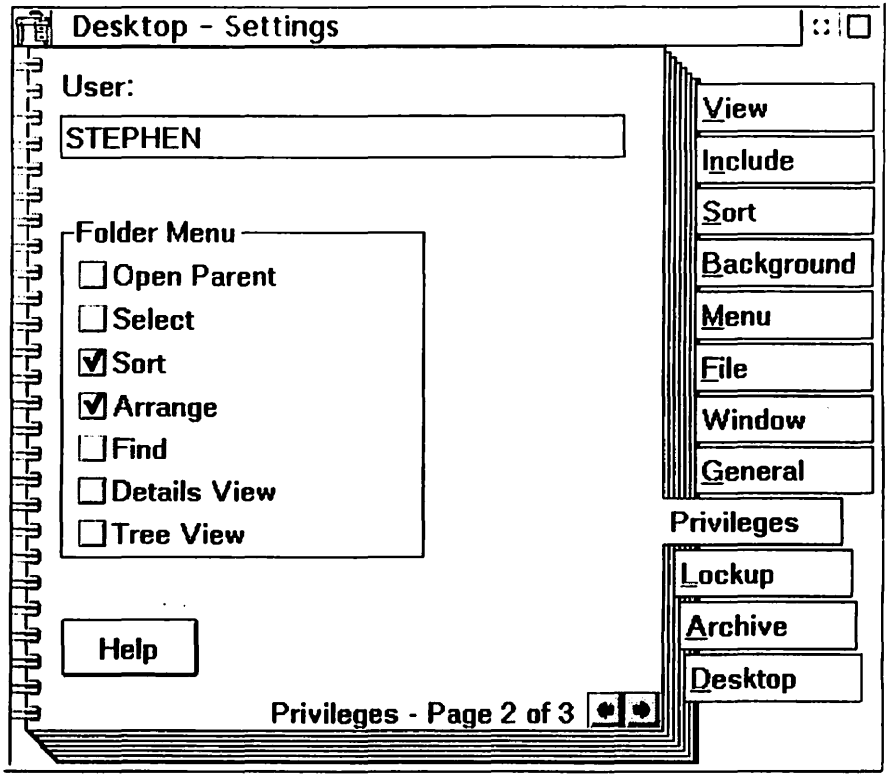
Attribute
Check this box to let the user change the file attributes. Deny this privilege to prevent the user from changing file attributes. This permission is enforced by the file access control driver. If you deny this privilege, we may also elect to omit the File tab from the object's settings notebook.

Create
Remove the check mark on this box to deny user access to the **Create Another...** item in the object's pop-up menu. With this permission removed the user cannot use the popup menu to create another object.

Help
Check this box to grant user access to the Help item on the object's pop-up menu. Denying this privilege does not prevent the user from gaining access to the help system through some other avenue.

Folder menu Privileges

The folder menu privilege page lets you assign user privileges for folder pop-up menu items. Each checkbox controls a different pop-up menu item. The folder menu **privilege** page is added to the settings notebook of every folder object in your workplace including desktops, file directories, and disks.



These items behave as follows:

Select
Check this box to grant user access to the **Select** item in the folder's pop-up menu. Deny this privilege to prevent the user from selecting or deselecting all objects in the folder. It does not prevent object selection with the mouse.

Sort
Check this box to grant user access to the **Sort** item in the folder's pop-up menu. Deny this privilege to prevent the user

from manually sorting the objects in the folder. This privilege does not override the "Always maintain sort order" settings in the sort page of the settings notebook.

Arrange
Check this box to grant user access to the **Arrange** item in the folder's pop-up menu. Deny this privilege to prevent the user from rearranging the objects in the folder.

Find
Check this box to grant user access to the **Find...** item in the folder's pop-up menu. Deny this privilege to prevent the user from performing find operations from the pop-up menu. The Find option is non-lethal. Even if a user can find the object, basic privileges will still be enforced.

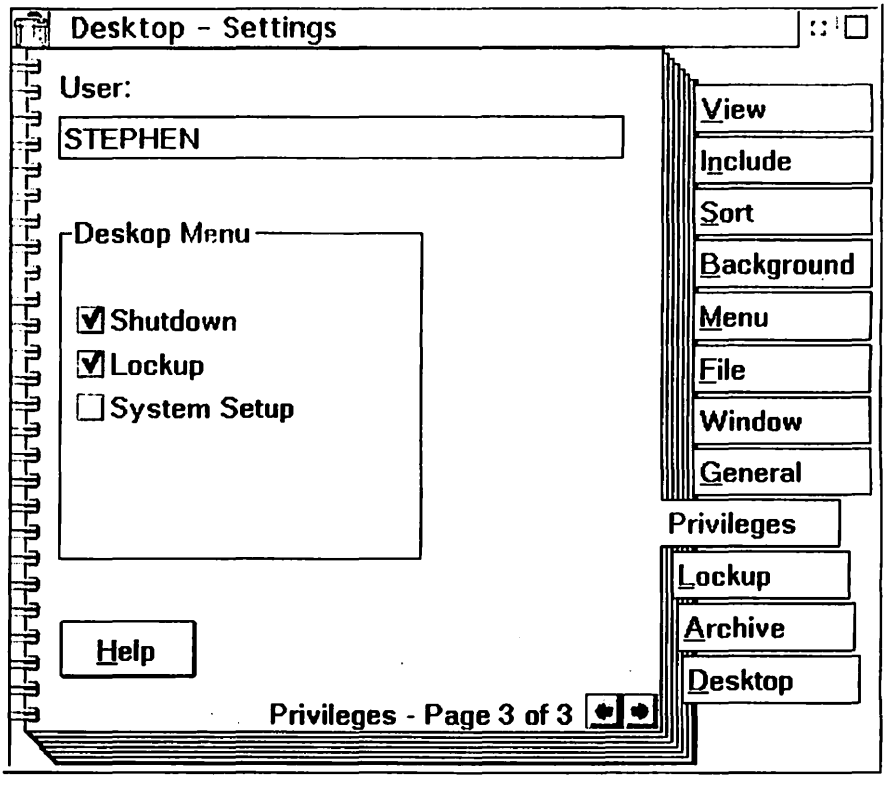
Details view
Check this box to allow the user to open a folder's Details View. Remove the check to prevent the user from opening the object's details view.

Tree view
Check this box to allow the user to open the folder's Tree View. Remove the check to prevent the user from opening the Tree view.

Open Parent
Check this box to grant user access to the **Open Parent** pop-up menu item. Remove the check to prevent the user from opening the folder's parent. The parent's open privilege will be enforced.

Desktop menu Privileges

The desktop menu privilege page lets you assign user privileges to pop-up menu items that are unique to a desktop. Each checkbox controls a different pop-up menu item.



These items behave as follows:

Shutdown

Check this box to grant user access to the **Shutdown** item in the desktop's pop-up menu. Deny this privilege to prevent the user from performing a system shutdown from the desktop pop-up menu. You can still perform a system shutdown with the SHUTDOWN.EXE program provided with The Secure Workplace.

Lockup

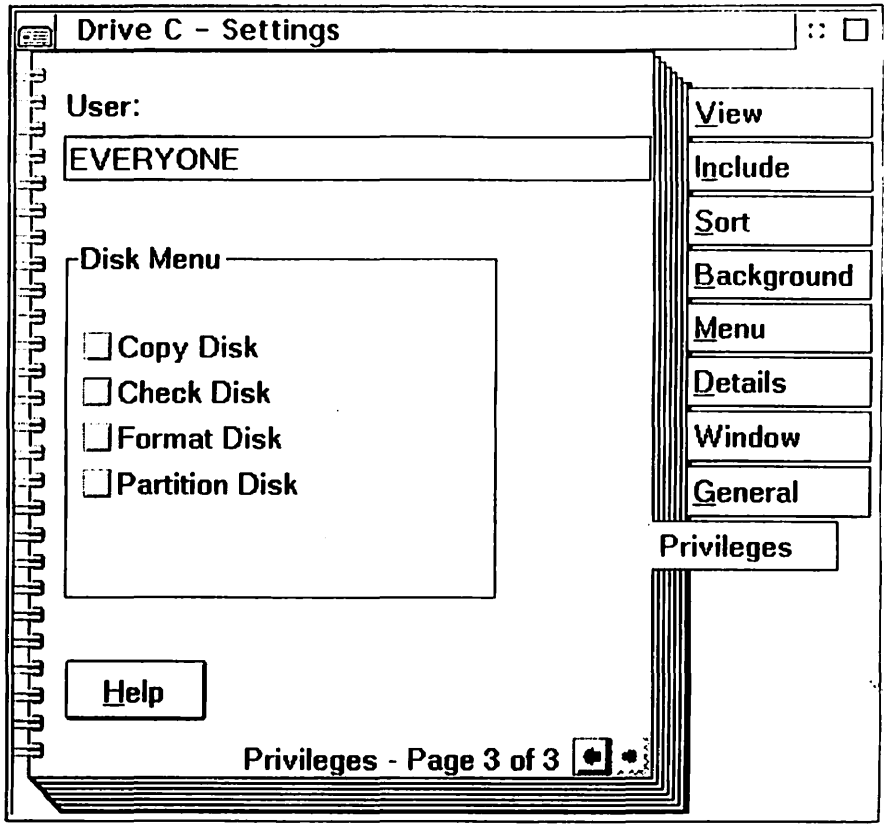
Check this box to grant user access to the **Lockup Now** item in the desktop's pop-up menu. Deny this privilege to prevent the

user from manually locking the desktop. This privilege does not override the Lock on startup or Automatic lockup settings in the lockup page of the settings notebook. The Lockup item can be used to activate The Secure Workplace screen saver.

System Setup
Check this box to grant user access to the **System Setup** item in the desktop's pop-up menu. Deny this privilege to prevent the user from gaining access to the system setup folder from the desktop's pop-up menu. This privilege does not override any privilege you assign to the system setup folder or its parent folders.

Disk menu privileges

The disk menu privilege page lets you assign user privileges to pop-up menu items that are unique to disk objects. Each checkbox controls a different pop-up menu item.



The disk menu privilege items behave as follows:

Check Disk
Check this box to grant user access to the **Check Disk** item in the disk's pop-up menu. Deny this privilege to prevent the user from performing a check disk from the pop-up menu.

Format Disk
Check this box to grant user access to the **Format Disk** item in the disk's pop-up menu. Deny this privilege to prevent the user from performing a format disk from the pop-up menu.

Copy Disk
Check this box to grant user access to the **Copy Disk** item in the disk's pop-up menu. Deny this privilege to prevent the user from copying disks.

Partition Disk
At the time of this writing this privilege is not available to users. Besides, the Drives folder usually contains this option. Only administrators can access this menu option.

Adding a User Privilege

Follow the procedure below to add a user privilege to an object.

1. Open the object's settings notebook.
2. Turn to the Privilege tab.
3. Bring up the user list by pressing the drop down button to the right of the user entry field.
4. Select the user or group that will receive the privilege. Users have a prefix of (U), and groups have a prefix of (G).
5. Check the privileges you want to grant.
6. If Page 2 exists, turn to page 2.
7. Check the folder menu privileges you want to grant.
8. If page 3 exists, turn to page 3.
9. Check the privileges you want to grant.
10. Return to page 1.
11. Press the Add button.
12. Repeat this procedure for each user user or group who will be granted a privilege.

Changing a User Privilege

Follow the procedure below to change a user's privilege to an object.

1. Open the object's settings notebook.
2. Turn to the Privilege tab.
3. Bring up the user list by pressing the drop down button to the right of the User entry field.
4. Select the user or group that will receive the privilege. Users have a prefix of (U), and groups have a prefix of (G).
5. Check the privileges you want to grant.
6. If Page 2 exists, turn to page 2.
7. Check the folder menu privileges you want to grant.
8. If page 3 exists, turn to it.

9. Check the menu privileges you want to grant.
10. Return to page 1.
11. Press the Save button.

Deleting a User Privilege

Follow the procedure below to delete a user's privilege to an object.

1. Open the object's settings notebook.
2. Turn to the Privilege tab.
3. Bring up the user list by pressing the drop down button to the right of the User entry field.
4. Select the user or group from the drop down list. Users have a prefix of (U), and groups have a prefix of (G).
5. Press the Delete button.
6. Repeat this procedure for each user whose privilege you want to delete.

Simple instructions for granting User Privileges

These instructions are intended to get you started quickly and to demonstrate a simple but effective security policy. You can use the environment or expand it to fit your needs.

1. Sign on as an Administrator.
2. Open the Security Administration notebook and turn to the Policy page.
3. Remove the check mark from the Grant public privilges by default box.
4. Configure any other policies you require. The Screen Saver is a handy feature to select.
5. Turn to the User tab.
6. Add at least one administrator.
7. Add as many users as you require. Skip this step if you decide to use Single Sign-on. If you are working with a notebook computer then add users who can take the notebook away.
8. Turn to the Groups tab.
9. Add a group that includes everyone. Lets say you called the

group EVERYONE. This EVERYONE group includes all users even ones that have not been defined yet. It includes users that are authenticated by your Single Sign-ON procedure, but who do not have a local definition.

10. Close the Security Administration notebook.
11. Open the Desktop settings notebook.
12. Turn to the Privileges Tab.
13. Select the EVERYONE group (ie.(G)EVERYONE).
14. Grant Visible, Open, and Execute Privileges on page 1.
15. Grant Sort and Arrange on page 2.
16. Grant Lockup and Shutdown on page 3.
17. Return to page 1 and press the Add Button.
18. Close the desktop settings notebook.
19. Open the OS/2 System folder's settings notebook.
20. Turn to the Privileges Tab.
21. Select the EVERYONE Group.
22. Deny all Privileges and press the Add Button.
23. Move all objects you want to protect into the OS/2 System folder. Be sure to move The Secure Workplace folder. and the Command Prompts folder into the OS/2 System folder.
24. You are done.
25. Test the configuration by signing on as different users.

The OS/2 System folder will be invisible to everyone except administrators.

Adding Launchpad Restrictions

Althought these instructions are optional, you might find them convenient.

1. Open the Launchpad settings notebook and turn to page 2 of the options tab.
2. Select the "Do not display actions" button.
3. Close the launch pad notebook.
4. Open your CONFIG.SYS file with the system editor.
5. Remove the LAUNCHPAD option from the AUTOSTART line.
6. Save the CONFIG.SYS file.

7. Reboot your computer.

Adding a Group with additonal Privileges

The procedure above created two groups of users. These are Administrators and everyone else. Suppose you have a third group that needs additonal privileges you do not want to grant to EVERYONE. Here is a procedure you can expand on:

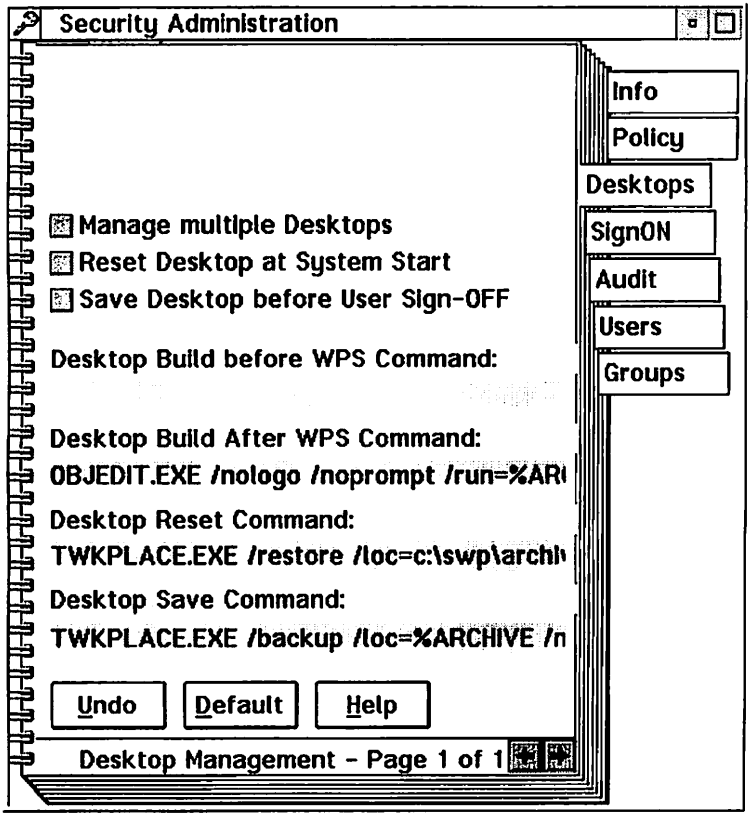
1. Open the Security Administration notebook and turn to the Groups tab.
2. Add a group that includes only the users you want to work with. Lets call this group SUPERUSERS for want of a better name. You can make-up your own name to fit your requirements.
3. Create a folder that will contain the objects SUPERUSERS can access. Lets call the folder **SupersOnly.**
4. Move what-ever objects the SUPERUSER group needs into this folder.
5. Open the **SupersOnly** settings notebook.
6. Turn to the Privileges Tab.
7. Select the SUPERUSER group.
8. Grant Visible, Open, Execute, Sort and Arrange privileges.
9. Press the Add button.
10. Select the EVERYONE group.
11. Deny ALL Privileges.
12. Press the Add button.
13. Close the settings notebook.
14. You are done.
15. Test the configuration.

When a member of the SUPERUSER group signs-on the **SupersOnly** folder will be visible. When any other user signs-on the folder will be invisible.

Multiple Desktop Management

Use the **Desktops** page in the Security Administration notebook to configure you system for multiple desktop management. If you purchased an Enterprise license then all items on this page can also be configured by running the setup program (SSETUP.EXE) with a response file.

The settings on the Desktop page (shown below) allow such flexibility that it would be difficult to fit all your options in this document. You should take note that the actual movement of desktops are controlled by programs that run in the background. We supply the Traveling Workplace to do this work. You can also use a third party product or write your own program as long as it fits inside the scheme we have provided.



Here are your options:

Manage multiple desktops

Check this box to activate multiple desktop management. When you check this box the CONFIG.SYS file is updated. You must shutdown and restart the workstation for the changes to take effect. On the next and subsequent system startups the SWMANAGE.EXE program runs before the Workplace Shell is invoked. SWMANAGE.EXE allows the user to sign-on, it executes the desktop management commands, and starts the workplace shell.

Save Desktop when User Signs off

Instructs The Secure workplace to run the Save desktop command just before signing the user off. Check this box if you want to permit users to change their desktops and to save these changes. If you decide to use the Traveling Workplace switching strategy then this is not necessary. Be sure to enter and test the save command.

Reset Desktop at Startup

Instructs The Secure Workplace to run the Reset Desktop command when the System starts and before a user signs-on. If you want to ensure that the system starts with the same default desktop this is a good idea. The reset command might wipe out any desktops left behind by the last user. The reset command should rely on resources local to the workstation because it occurs before user sign-on. You can use Traveling Workplace to backup a desktop into an archive directory on a local hard drive, Then enter a Reset command to restore this local desktop. The restored desktop should be small enough to be restored quickly. It might have enough resources to allow an administrator to perform maintenance or it might have resources to allow a user to work at the workstation when the network is down. Your might also want to consider this desktop for notebook computers that are intermittently disconnected from from your network.

Desktop Build Before WPS Command

Enter a command to be executed before the Workplace shell is started. If you leave this field blank then the active desktop is

used. Press the defaults button to get the Traveling Workplace /RESTORE command. You can also use the Traveling workplace /SWITCH or /NEW strategy options here.

Desktop Build After WPS Command
Enter a command to be executed after the Workplace Shell is started. If you leave this field blank then nothing happens. Press the defaults button to get the default Object Editor command.

Desktop Save Command
Enter a command to be executed just before the user signs off. Press the defaults button to get the default Traveling Workplace /BACKUP command. This command will not be invoked unless you check the **Save Desktop when user signs off** option.

Desktop Reset Command
Enter a command to be executed when the system starts and before a user is allowed to sign on. Press the defaults button to get the Traveling Workplace /RESTORE command. This command will not be invoked unless you check the **Reset Desktop at System Startup** option.

Specifying Commands

In the Security Administration notebook, the Desktop Management and User Signon configuration pages ask you to enter commands that will be executed at appropriate times. The commands specify programs and program parameters that execute in the background without user interaction. For instance Syntegration Inc. Supplies programs such as Traveling Workplace (TWKPLACE.EXE), Object Editor (OBJEDIT.EXE) and System Setup (SSETUP.EXE) that can operate in a non-interactive mode. You can also write your own REXX program or batch file to perform the required tasks.

Commands consist of a program file name followed by program parameters. The program file name consists of the filename and extension. Examples of valid program file names are CMD.EXE, TWKPLACE.EXE, OBJEDIT.EXE, and SSETUP.EXE. File names without extensions are invalid. Examples of invalid program file names are CMD, TWKPLACE, OBJEDIT SSETUP. If the program file does not reside in a directory in the PATH, the

program name should be fully qualified. An example of a fully qualified program file is C:\SWP\BIN\TWKPLACE.EXE

Program parameters are used by the program to tell it what to do. Parameters are separated from the program file name by a space. You should also separate multiple parameters by spaces to insure that the program recognizes them correctly. You can specify substitution keywords in commands. These keywords will be translated by The Secure Workplace before executing the command. For example, %USER will be translated to the UserID entered when a user signs-on.

The substitution keywords are:

Keyword	Description
%USER	The user ID as entered at login.
%PASSWORD	The password as entered at login.
%LOGFILE	The current log file name.
%STATION	The station name assigned to the computer.
%ARCHIVE	The User's Archive directory.
%CLASS	The User's Class name.
%NEWPWD	The User's new password for password changes.
%REMOTE	The UPM Remote or Domain name.

You should note that user specific keywords are not available before a user signs on.

If you use a REXX command or batch file to perform a procedure it must be invoked by the CMD.EXE program with the /C parameter. An example REXX command follows.

```
CMD.EXE /C RESTORE.CMD %ARCHIVE
```

In this example the, RESTORE.CMD file is executed with the user's archive directory as its sole parameter.

User's Guide

The Secure Workplace for OS/2 is a workstation security and desktop management system that was installed and configured by your system administrator.

When the system starts you will be asked to enter your user-ID and password. This information may also be used to login to a network or remote host.

After you sign on the product can provide you with your own desktop. This desktop may be share by all users, It may be shared by a group of users, or it may be unique to you. The system administrator may allow you to make changes to this desktop.

The product includes a screen saver feature that will lock the keyboard after a period of inactivity. Use your sign-on password to unlock the computer when ever the screen saver is invoked.

The system can be configured to keep track of your activities in a special audit log. This allows for maximum system security. The audit log may also be used to track desktop management problems.

We have provided you with this guide to help you understand how to use the system. Refer to the following sections for further information:

Signing on to the System
Changing your password
Operating the Screen Saver
Signing out of the System

Signing on to the System

When you start up your computer, and after you sign-off the Secure Workplace may display a user sign-on window that will prompt for a user identification and password. The system administrator will assign you with a user name consisting of any alphanumeric combination of up to 15 characters. Your will also be assigned an initial password again consisting of any alphanumeric combination of up to 15 characters.

The administrator may or may not require you to enter your password at start-up. In this case the system may be configured for auto sign-on as a guest user. If your are presented with a sign-on window or the screen is blank then follow the procedure below to sign-on.

1. If the screen is blank, bring up the desktop pop-up window with your keyboard or mouse.
   a. With the mouse press the right button.
   b. With the keyboard press <SHIFT+F10>
   c. Select either the "Logon..." or "Logoff..." item.
2. A period of activity may occur as the system resets or saves the current desktop. The user sign-on window should now appear.
3. Use your mouse or <Tab> key to put the cursor at the User ID entry field, then enter your assigned user name.
4. Press the <Tab> key or use the mouse to select the password entry field. Do not use the <Enter> key to make the transition because this will prematurely start the sign-on process. The field will display asterisks in place of your password to prevent onlookers from obtaining your password.
5. If the remote name field is available and the system administrator has given you instructions on what to enter then enter a remote name. This field is not normally

required so do not worry about it.

6. Press the Logon button or the <Enter> key to start the sign-on process.
7. The progress window will tell you if the user-ID and password you entered was valid. After successful sign-on the OK button will become enabled.
8. Press the OK button to dismiss the sign-on window and to gain access to the system.
9. A period of activity may occur as the system restores your desktop.

The system administrator may allow you to sign-on locally at the workstation, or to a network or remote host computer. In case the network or host system is down you may want to sign-on locally to use your computer in a stand alone mode. If this is the case, and the local sign-on check box is available to you, check it before pressing the Logon button.

The system will alert you when your password is about to expire. Refer to the section titled "changing your password" for instructions.

Changing your Password

The administrator may decide to limit the number of times you can sign-on with the same password. The system will display messages in the sign-on window to alert you when to change your password. If you allow your password to expire you will no longer have access to the system.

The system administrator may or may not permit you to change the password yourself. If you are not authorized to change your password, notify the system administrator before the password expires. If you are authorized, then follow the procedure below to change your password.

1. Bring up the user sign-on window. You can do this by

signing-off or by restarting the computer.

2. Type in your user name then press the <Tab> key to move to the password field.
3. Type in your current password.
4. Press the <Tab> key until the change password box is selected, then check the box with the space bar. You can alternatively click this box with the mouse.
5. Two new entry fields will appear. Use the <Tab> key to move the cursor to the new password entry field
6. Type in your new password then press the <Tab> key again to move to the Twice field.
7. Type in your new password again for verification.
8. Press the <Enter> key or the Logon button.

The system administrator may have specified a minimum password length. You must comply with this policy. If you fail to comply, the system will alert you to the minimum length. The maximum lenght is 15 characters. Your new password will remain valid until you change it, or until the password expires.

Operating the Screen Saver

The administrator may have selected a security policy that invokes a screen saver after a specified period of inactivity. This policy can protect sensitive information from being seen on an unattended workstation, prevent running programs from being stopped, and prevent unauthorized keyboard entry. Your administrator may allow you to invoke the screen saver yourself.

When the screen saver is activated the computer system will continue to work and the programs are still executing but the keyboard is locked to everything except password entry. The screen may be blanked, a lockup bitmap may be displayed, a lock icon may be floating around, or a small window may be alerting you that the system is locked.

To unlock the system after the screen saver is activated you must either:

1. Re-enter your sign on password.
2. Power down and restart the computer.
3. Type "LOGOFF" to sign-off the previous user and restart the sign-on sequence.
4. Contact your system administrator for a dynamic password.

When the screen saver is active and the keyboard is locked you cannot reboot the computer with the <CTRL+ALT+DEL> keyboard combination.

To invoke the screen saver prior to automatic lockup.

1. Move the mouse to an open area on your desktop.
2. Press the right mouse button to get the desktop pop-up menu..
3 Select the "Lockup Now" menu item.

Signing off the System

After you finish working on the system you have to sign-off to prevent others from accessing the computer system under your name. To sign off you may use one of the following procedures:

Shutdown the system

1. Bring up the desktop pop-up menu by clicking the right mouse button on any open area of the desktop.
2. Select the Shutdown item.
3. Wait until the system prompts then power off the computer.

Logoff

1. Bring up the desktop pop-up menu.
2. Select the Logoff... item.

Activate the screen saver

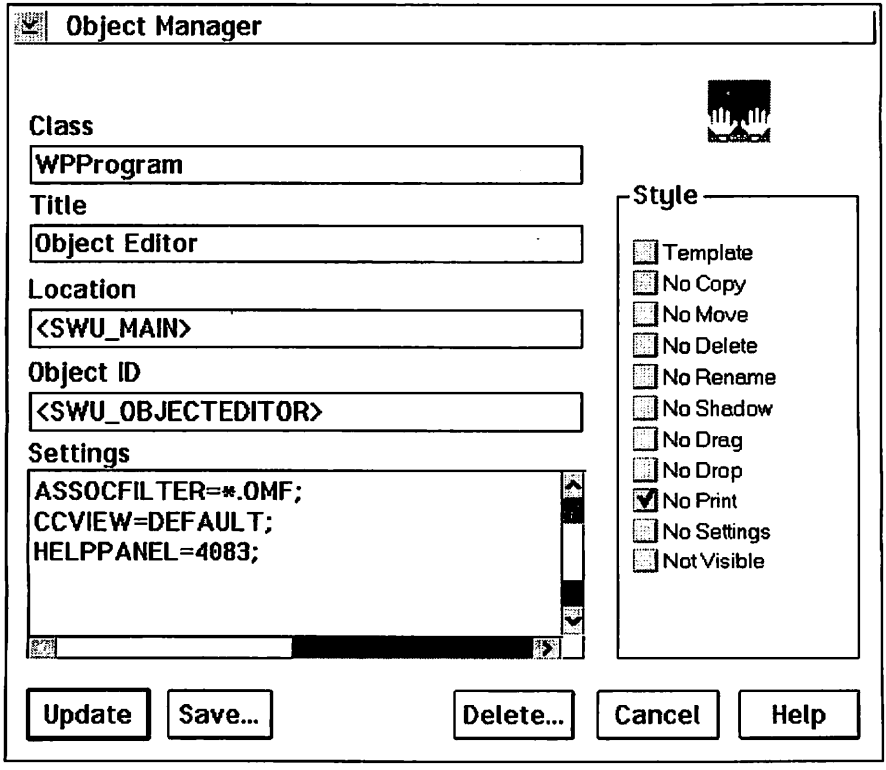
1. Bring up the desktop pop-up menu.
2. Select the Lockup Now item.

Object Manager

The Object manager is a workplace class object (SWObjMan) used to allow you to query, save, and update the settings of any workplace object. You can also destroy objects. You initiate the object manager by dropping another object on it. This tool can be used in conjunction with the object editor.

The Object Manager is intended for administrative use. You should not deploy this object in a secure end user environment.

When you drop a workplace shell object on the object manager the dialog box below appears. The Object managers queries the dropped object and displays its class, title, location, and settings.



You may update the object by making the desired changes and pressing the "Update" button.

The "Save..." button allows you to backup the object into an object make file format. If the object is a folder the object managers will also save its contents. When you attempt to save over an existing file the object manager gives you the option of overwriting or appending to the file. Once you save the object, you can make changes with a text editor or the Object Editor. Use the Object Editor to rebuild saved objects.

The delete button allows you to destroy the object you dropped. If the object is a folder its contents will also be destroyed.

Object Editor

The Object Editor (OBJEDIT.EXE) is an alternative to the interactive drag and drop method of object creation provided by the Templates folder. This utility is a powerful tool for bulk object management.

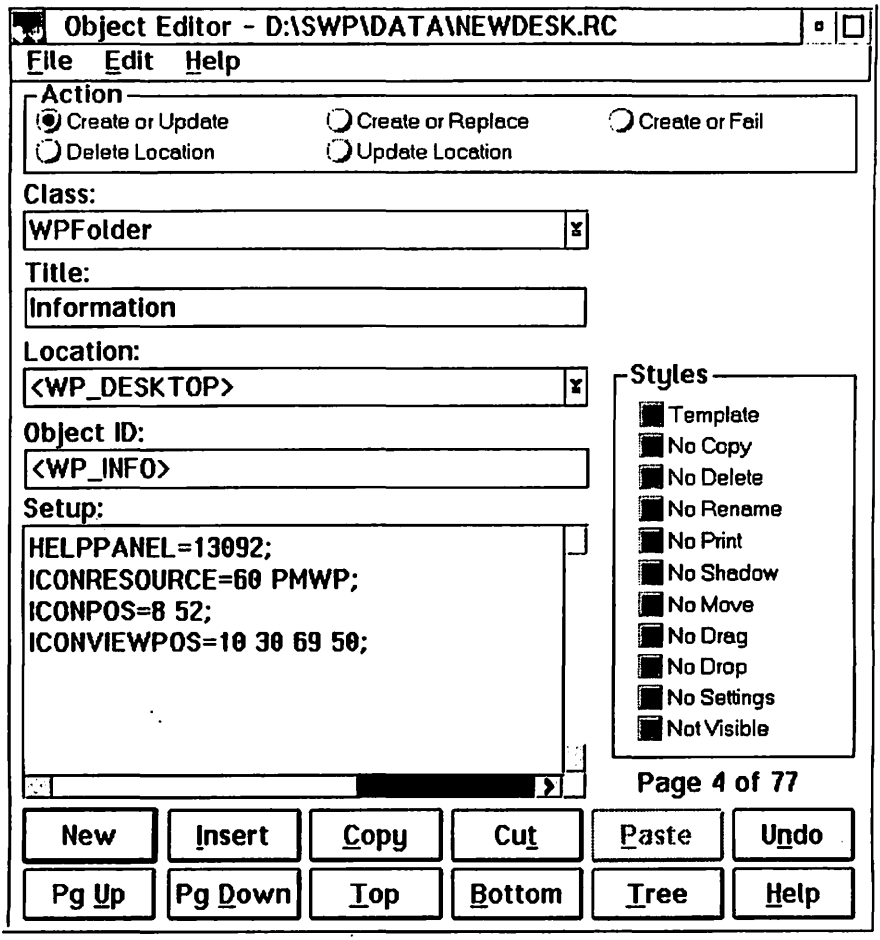
The Object Editor lets you create and edit a list of actions that can be performed against workplace shell objects. You can use these actions to create objects, delete objects, or change an object's settings. With this capability, you no longer have to write REXX programs in order to customize and build Workplace shell objects in an unattended fashion.

Once you have built a list, you perform the actions in sequential order by selecting the **File / Run** menu option. You can also perform the actions in the object list automatically when you start the Object Editor with the /RUN start-up parameter.

Object action lists are stored in object make files (*.OMF). Object Make files are regular ASCII text files. These files can also be edited with any text editor such as the System Editor or the Enhanced Editor that comes with OS/2. Object make files are created by the Object Manager when it saves objects.

To restate its capabilities, you can use the Object Editor to:

- Edit and restore objects saved by the Object Manager.
- Populate a desktop with new objects.
- Update workplace object settings.
- Delete workplace objects.
- Perform all the above in an unattended fashion.
- Import object definitions from a desktop resource file (ie. INI.RC)
- Export object definitions to a desktop resource file (*.RC)



Use the Object Manager's save function to save a list of objects into an object make file. After the list is created, use the Object Editor to make insertions, deletions, and changes. Once your modifications are complete use the editor to rebuild the objects in the list.

The Object Editor command line syntax is:

OBJEDIT *[options]*

The available options are:

filename	Object make file containing a list of objects and actions to be performed.
/NOLOGO	Do not display the initial logo screen

/LOG[=lFile] Log all operations to the specified logfile. If no log file is specified the program will write to OBJEDIT.LOG in the current directory.

/HOME Allows you to specify an OBJECTID on the command line. The object editor will substitute the OBJECTID in the LOCATION or SETUP strings where it finds the keyword "<HOME>"

/RUN[=RFile] Specifies that the actions described in the object list should be performed. if *RFile* is specified then it is assumed to contain the object list.

An Object Make File (OMF) contains keywords that correspond to the parameters of the REXX SysCreateObject function. These keywords are CLASS, TITLE, LOCATION, SETUP, and ACTION.

The following example shows the format of an Object Make File. Blank lines are ignored.

```
CLASS      "WPFolder"
TITLE      "The Secure Workplace Utilities"
LOCATION   "<WP_DESKTOP>"
SETUP      "OBJECTID=<SWU_MAIN>;LOCK=YES;"
ACTION     U

CLASS      "WPProgram"
TITLE      "Object Editor"
LOCATION   "<SWU_MAIN>"
SETUP      "EXENAME=objedit.exe;PROGTYPE=PM;"
SETUP      "OBJECTID=<SWU_SCMDPROMPT>;"
ACTION     R

LOCATION "<SWU_MAIN>"
SETUP    "DETAILSVIEW=FLOWED"
ACTION   E
```

Refer to the chapter titled "Customizing Workplace Objects" for more information and a detailed explanation of these keywords. The SETUP keyword can be specified multiple times for each ACTION. Each time a SETUP keyword is encountered, the parameter is concatenated to the existing setup string.

The ACTION keyword can specify the following actions:

F To create a new object or Fail if an object with the given OBJECTID exists.

R To create a new object or replace any existing object with the given OBJECTID.

U To create a new object or update the settings of any existing object with the given OBJECTID.

D To delete the object with OBJECTID specified by the LOCATION. The CLASS, SETUP, and TITLE keywords are ignored when the delete action is specified.

E To call SysSetObjectData with OBJECTID specified by the LOCATION and Setup string specified by SETUP. This action updates an existing object's setup data. The CLASS, and TITLE keywords are ignored when this action is specified.

Avoid the following sequence because it will delete all deletable objects on your desktop.

```
LOCATION    <WP_DESKTOP>
ACTION      D
```

System Shutdown

The system shutdown utility (SHUTDOWN.EXE) provides a way to control the shutdown process. With this program, you can shutdown your workstation from the command line, a batch file, a REXX program, or by double clicking the mouse on a program object. You can also use this tool to customize your system shutdown procedure.

The command line syntax for the Shutdown utility is:

SHUTDOWN [/NOLOGO] [/NOPROMPT] [/DELAY=n]

Where:

/NOPROMPT	causes the program to bypass the confirmation dialog box.
/NOLOGO	causes the program to bypass the initial logo screen.
/DELAY=n	causes a delay of n seconds before the shutdown proceeds.

Window List Manager

The Window List Manager (WINLISTM.EXE) provides a way to control entries in the Window List. With this program you can :

- Exclude program items from the window list. Removing a program item from the Window List means that the user can not switch to that program by use of the <Alt> + <Esc> hot key.
- Prevent the user from closing specified programs from the window list. This is achieved by making these program items invisible in the window list while still allowing use of the <Alt> + <Esc> hot-key to switch to the program

One example which demonstrates the control potential of this utility is, for instance, where an OS/2 system is running a mission critical application and the application is required to be in the foreground at all times. You can use the window list manager to remove all items except those titles that will not disrupt the process.

The syntax is:

WINLISTM [*/NOLOGO*] [[[*/A*] | [*/R*]] [*filename*]]| [*/I*]

Where:

/A	Remove all program items NOT found in the data file. If this option is specified then the *filename* must also be specified.
/R	Remove the program items found in the data file. If this option is specified then the *filename* must also be specified.
/NOLOGO	Do not display the initial logo screen
/I	Run the window list manager in interactive mode. If this option is selected all options except the */NOLOGO* option is ignored.
filename	Data file containing a list of window list titles to be operated on.

Notes.

The */A* and */R* options are mutually exclusive.

If the program is started with no parameters, it will remove all entries from the Window List.

Each entry in the data file occupies a single line in the file. The entry will contain a *Command Parameter* and an *Entry Title. Entry Titles* are treated as partial titles. A match will occur if the specified title matches part of the text of an entry in the Window List. This provides an easy way to remove several similarly named entries. *Command Parameters* are described below.

Parameter	**Description**
C	Do not allow the item to be closed from the window list. The user can still switch to the item with the <ALT>+<ESC> hot-key.
N	Normal operation depending on the */A* or */R* startup option.

Any line starting with a semi-colon is treated as a comment and ignored.

In a production environment, the window list manager should be started by putting a command line in the STARTUP.CMD or by placing a window list manager program object in the <WP_START> folder.

Examples:

The following example demonstrates the format for a data file. The first three lines are comments. The fourth and fifth lines tell the window list manager to take the normal action on any item with "Desktop" or "Server" in the title.

```
;FILE: WINLIST.DAT
; Sample file to remove desktop object from the switch list
;
N "Desktop"
N "Server"
```

The command line below invokes the window list manager to remove the programs with titles in the WINLIST.DAT data file.

```
WINLISTM /R WINLIST.DAT
```

The data file contents listed below illustrates a system which will allow you to run a set number of applications. As before, the first line is a comment. The second line will allow a matching program to come to the foreground by using the <ALT> + <ESC> hot-key. (Such a matching program will not be visible and cannot be closed from the window list.) The normal action will be taken on items that match the title in the third line.

```
; FILE: WLMALLOW.DAT
C "My Critical Application"
N "My Secondary application"
```

The command line below invokes the window list manager to allow programs with titles in the WLMALLOW.DAT data file to appear in the window list. The /NOLOGO option causes the window list manager to bypass the logo screen.

```
WINLISTM /A /NOLOGO WLMALLOW.DAT
```

The command line below is an example instruction to place in your STARTUP.CMD file.

```
START WINLISTM /A /NOLOGO WLMALLOW.DAT
```

Desktop Management Strategies

As we said before, with The Secure Workplace your desktop management options are innumerable. The following is a list of strategies that employ tools we supply or support.

Users see different views of the same Desktop

This is perhaps the simpliest, safest, and fastest strategy because the desktop remains the same. This strategy can be employed without the use of any additional tools. By assigning user privileges to desktop objects you can let users see only the objects they have permission to use. See the section titled "Simple instructions for granting user privileges" for details. If you want to update the desktop periodically or provide additional insurance against changes then:

1. Open the Security Administration notebook and turn to the Desktops tab.
1. Check **Multiple Desktop Management**.
2. Uncheck **Reset Desktop at Startup**.
3. Uncheck **Save Desktop when user signs off**.
4. Remove the **Desktop Build After WPS command**.
5. Enter a **Desktop Build Before WPS Command** to restore the desktop from a local or network archive. If you choose to restore from a network archive then you can periodically update the desktop without going to the workstation.

Switching between on-line Desktops

Use the Traveling Workplace switching strategy to switch between on-line desktops that reside on the local workstation. This strategy is invoked by the the Traveling Workplace / SWITCH option. Switching is usually much faster than restoring. However it will not allow a user to move from one workstation to another and get the same desktop every time. We recommend this option if you have a limited number of desktops, users do not move between workstations, and speed is essential. You must setup pre-existing desktops before invoking this strategy. See the Traveling Workplace reference manual for

details. Here are some basic instructions.

1. Refer to the Traveling Workplace Reference for details. Pay special attention to the sections on multi-user setup.
2. Start Traveling Workplace. and select an Archive directory.
3. Open the Traveling Workplace preferences window. Disable the cleanup after restore option, disable the re-use default names option, and disable the Update CONFIG.SYS Option. Set the number of on-line workplaces to the number of desktops you will support.
4. Backup the desktop into the archive directory.
5. Restore the Desktop from archive to build a new desktop (ie.Desktop0).
6. Create as many desktops as you will need.
7. Switch between desktops and remove or add objects to fit each user or user group needs.
8. Test the Traveling Workplace /SWITCH command from a command prompt to develop a set of parameters to fit your needs.
9. Open the Security administration notebook and turn to the Desktops tab.
10. Check the **Manage Multiple Desktops** option.
11. Uncheck the **Save Desktop at user sign off** option
12 Uncheck the **Reset Desktop at System Startup** option.
13 Enter the Switch command you developed into the **Build Before WPS command** field.
14 Define User class names to represent each desktop you will support. User Class names are defined on Page 3 of the User Definition Tab. Use Class names like "Desktop0", "Desktop1", "Desktop2", etc. These names are the names available with the Traveling Workplace /DESKTOP parameter.

Restore Desktop from archive

Use the Traveling Workplace restore strategy to update the desktop for each user or user group that signs-on to the workstation. This is your most flexible strategy. It is designed to be used with the Traveling Workplace /RESTORE option.

You can restore a desktop from an archive directory that resides on the local workstation or on a network file server. With this option you can let a user move between workstations and get the same desktop every time. If the archive directory is on a file server then you can dynamically update the restored desktop withour having to take a trip to the workstation. You can allow a user to save changes by adding a Save Icon to the restored desktop. This Save Icon could invoke Traveling Workplace with the /BACKUP option. We recommend this strategy when you have a large number of users, Users share workstations, users move between workstations, Workstations are networked, you want maximum assurance that desktops remain the same, you want to dynamically update the desktop. We believe the restore strategy will be faster than the build strategy but slower than the switch strategy. See the Traveling Workplace reference manual for further details. Here are some basic instructions.

1. Refer to the Traveling Workplace reference for details. Pay special attention to the sections on multi-user setup.
2. Start The Traveling Workplace.
3. Open the Traveling Workplace preferences window. Disable the cleanup after Restore option, disable the re-use default names option, Disable the Update CONFIG.SYS option, and set the number of on-line workplaces to any number that will fit on the local hard drive.
4. Select an Archive Directory for the user or user group.
5. Backup the Desktop into the archive directory.
6. Restore the Desktop from archive to build a new desktop.
7. Configure the desktop for the user or group. You achieve this by adding or removing objects to fit the user's needs.
8. Backup the new desktop into the archive directory.
9. Repeat these steps for each user or user group.
10. Test the Traveling Workplace /RESTORE command from a command prompt to develop set of parameters to fit your needs. You will want to use the /NOUPDATE parameter to prevent the CONFIG.SYS from being changed.
11. Open the Security Administrarion notebook and turn to the Desktops tab.
12. Check the **Manage Multiple Desktops** option.

13. Uncheck the **Save Desktop at user sign off** option
14. Uncheck the **Reset Desktop at System Startup** option.
15. Enter the Restore command you developed into the **Build Before WPS command** field. Use the %ARCHIVE substitution keyword with the /loc parameter (ie./ loc=%ARCHIVE).
16. Define an archive directory for each user or user class. Archive directories are defined on Page 3 of the User Definition Tab. The user's archive directory is used when you specify %ARCHIVE on the build command. The Traveling Workplace /LOC parameter is designed to accept an archive directory.

Special Note: The Traveling Workplace cannot change the desktop directory name with the /RESTORE option when it restores before the Workplace Shell starts. Instead the product uses the same desktop directory name that was assigned when the desktop was saved. This may have the side effect of replacing an existing desktop including the default or boot-up desktop. This effect is not necessarily a bad thing, but you should be aware that it can happen. Suppose a user signs on and his restore procedure fails because his archive directory was not available or empty. If the last user replaced the default desktop then the new user will get the last user's desktop. You can avoid this effect by ensuring the archived desktops uses a name other than the default desktop name. Here is a procedure that will help you to avoid this problem.

1. Start the Workplace Shell
2. Start the Traveling Workplace and switch to the default desktop. (\DESKTOP)
3. Turn off the Traveling Workplace Clean up after preference.
4. Remove all other on-line desktops from you system.
5. Backup and restore this desktop to create new desktop (\DESKTOP0)
6. Backup this desktop to the user archives.
7. Turn on Multiple desktop management and reboot you system to make it active.

Now every time a user signs on and restores with the Build Before WPS command the restore procedure replaces the \DESKTOP0 directory, OS20.INI file, and the OS2SYS0.INI.

Suppose you want assure yourself that the Traveling Workplace will never overwrite your default desktop. Use the workplace shell drive folder to change the default desktop directory name to something like DEFDESK. Copy the user and system profiles to a uniques name like DEF.INI and DEFSYS.INI. Update the CONFIG.SYS to use these unique names.

Build a new Desktop

Use this strategy when you want to dynamically create objects on a blank or minimally populated desktop. To do this you can specify a build before and a build after command. The build before command is executed before the workplace shell starts and the build after executes after the workplace shall starts. Use the build before command to create the desktop. Use the build after command to populate the desktop with objects. The Traveling Workplace /NEW parameter can create a desktop for you. The Object Editor can populate this desktop with objects.

User sees only Network Applications

In this scenario, you use IBM LANServer or IBM WARP Server and have already assigned network applications. You decide to use the User Profile Manager Domain for Single Sign ON. The user is not defined locally or you deny access to the desktop. In this scenario all local desktop objects are invisible. The Network applications folder and its contents are visible. Here are some basic instructions.

1. Turn off multiple desktop management.
2. Configure single sign-on for User Profile Manager Domain.
3. Remove all user privileges or set them such that the default desktop objects are invisible.

The Secure Workplace automatically leaves the Network Applications folder and its contents alone and lets your network operating system manage them.

Unattended Installation

If you are using The Secure Workplace in a stand-alone environment then it is safe to skip this chapter. If you manage many workstations in a remote or network environment then unattended installation and customization is an important issue for you. **The Secure Workplace for OS/2** contains utilities and features that will significantly reduce your labor in these environments. These tools will assist you with:

- Software Distribution.
- Security Administration.
- Desktop Management.

System Setup

The System Setup (SSETUP.EXE) program will run in an unattended mode if you specify the /S, /T, and /RSP command line options. You can specify a response file to competely install and/or configure the product. This response file capability is available when you purchase an Enterprise License. The System Setup program is your tool for unattended Software Distribution and Security Administration.

Object Editor

The Object Editor (OBJEDIT.EXE) will run in an unattended mode, if you specify the /RUN and /NOLOGO startup parameters. With this capability you can create, update, or delete one or more objects on a desktop. See the "Object Editor" and "Customizing Workplace Objects" chapters for details.

Traveling Workplace

If you specify the correct startup parameters, Traveling Workplace will run in an unattended mode and read a response file. Traveling Workplace will perform all multiple desktop management functions for you. In addition, Traveling workplace can perform some software distribution tasks when you specify additional files in the archive set. Traveling Workplace is included when you license the Professional Edition. You can also purchase Traveling

Workplace Separately. See the Traveling Workplace manual and the "**Customizing the OS/2 Workplace**" reference for details.

Network Updates

When you purchase an Enterprise license The Secure Workplace OS/2 will allow you to implement an automatic update of Users, Groups, and Privileges from the network directory. This update occurs just after the User Signs-ON. The network directory should be set for read-only access.

You should refer to the utilities available with your network operating system for additional information on unattended installation. LANSERVER (tm), for instance, includes utilities called CID. IBM publishes many REDBOOKS on the subject of OS/2 Configuration. One we recommend is "OS/2 Configuration Techniques: Cracking the Workplace Shell" (document number GG24-4201-00). This book is a valuable source of information for anyone who deploys Workplace Shell desktops in an unattended mode.

If you enroll in our **Maintenance and Support Services** offering we can assist you with developing a strategy for unattended installation and customization.

Using Response Files

The distribution diskette includes a sample response file (SSETUP.RSP). This file includes all the response file options you can use for unattended installation and customization. The on-line reference contains a copy of this file. If you are going to use unattended installation it is essential that you refer to the information contained within this file.

When you purchase an Enterprise license, the System Setup (SSETUP.EXE) program will accept a response file parameter on the command line that you can use to install the product and/or completely change the administrative settings. Use this program for unattended software distribution and security administration. The System Setup program requires Presentation Manager.

Therefore, you must install OS/2 before using it. Here are a few of the ways you can use the response file feature:

- With IBM NetView Distribution Manager/2.
- With the Redirected Installation and Configuration (CID) component of IBM LANServer or IBM WARPServer.
- With other Network Management or Software Distribution products.
- As part of logon script you develop to update the security settings.
- As part of a custom REXX program you develop to administer disconnected workstations or notebooks at remote locations.

Note: You can perform customization only operations by setting **"InstallFiles = NO"**, and **"BuildObjects=NO"**.

Setup Procedure

If you intend to install and configure The Secure Workplace in an unattended mode then the following procedure will get you started.

1 Create a subdirectory on your File Server or Code Server.
2 Copy all files from the distribution diskette(s) to the directory you created.
3 Modify the response file (SSETUP.RSP) to fit your requirements.
4 Add the SSETUP.EXE program with its start-up parameters to your software distribution procedure.

We leave it for you to decide on the best implement for your environment.

Using Network Updates

If you purchased an Enterprise license, The Secure Workplace can implement automatic updates from the network directory. The network directory is specified in the SWPNETPATH environment variable. The product updates User definitions, User Group definitions, and User Privilege assignments from the SECUREWP.INI file whenever a user signs-on. This capability

minimizes administrative labor by assigning a central location for distributing new user privileges. Here are some basic instructions:

1. Create a network directory and alias that will be visible to all users. Lets say that you assigned drive S: and directory S:\SWPADMIN
2. Grant read only access to the users.
3. When you install The Secure Workplace for OS/2 at the workstation, specify S:\SWADMIN as the network directory.
4. However you administer the workstation set the Security policy to Update User Information from Network directory.
5. Define users and privileges on your test or administrative Workstation.
6. Copy the Security Profile SECUREWP.INI to the network directory.
   Your local SECUREWP.INI file is usually hidden, read-only, and the contents are encrypted. This file is usually located in the install directory. The XCOPY command with the /H parameter can handle the movement of this file to the network directory. Once its in the network directory you can remove the hidden attribute with the ATTRIB command.
7. Update the SECUREWP.INI file in the network directory whenever you add a new user or change privileges.
8. We intend to simplify this process by adding import, export, and response file capabilities to the Security Administration program.

Customizing Workplace Objects

Workplace Shell objects are easily customized through their settings notebook. This approach is fine for the user. Administrators who need to customize one or more workstations in an unattended fashion require an alternative path. The information in this chapter will help you to customize and distribute objects in an unattended mode with a minimum amount of labor. Additional information is available in the "Customizing the OS/2 Workplace" on-line reference.

The OS/2 operating system provides an Application Programming Interface (API) for this purpose. You write compiled language or REXX programs to access these functions. You can find the API descriptions the Information Folder under REXX Information. Look in the Rexx Utilities chapter of the contents.

The Secure Workplace provides a tool, called the Object Editor, that gives you access to the Workplace Object API without forcing you to write a program. With the Object Editor you can create, modify, or delete OS/2 Workplace objects. Once you understand how objects are described, The Object Editor can help you to speed up the customization process.

Creating Workplace Objects

The easiest way to create a workplace object is by dragging the representative icon from the **Templates** folder. This method is convenient, but it does not provide the hands-off capability required for unattended customization.

To create an object you must first be able to describe it. An object is described by a **Classname**, a **Title**, a **Location**, and **Setup** parameters. These items are described below.

Classname

The type of object to be created. The **classname** is a case sensitive word such as WPProgram, WPFolder, WPPrinter, and others. You can get a list of available OS/2 Workplace classes

from the Object Editor class list.

Title

The object's title. This title appears below the object's icon and can also be modified in the general page of the settings notebook. You can define multiple line titles by using the carat character "^" as a line delimiter.

Location

The object's location. This item defines a folder in which the object will be placed. You can specify either an OBJECTID or a file system path. When you specify a path you must use a fully qualified path name such as "c:\desktop\information". An OBJECTID begins with '<' and ends with '>'. OBJECTIDs are defined later on. Some predefined OBJECTIDs are:

<WP_DESKTOP>	The Desktop.
<WP_START>	The Start-up folder.
<WP_OS2SYS>	The System folder.
<WP_TEMPS>	The Templates folder.
<WP_CONFIG>	The System Setup folder.
<WP_INFO>	The Information folder.
<WP_DRIVES>	The Drives folder.
<WP_NOWHERE>	The hidden folder.

Setup

A setup string containing a series of "keyname=value" pairs, that define the behavior of the object. "Keynames" are separated by semicolons, and "values" are separated by commas. The last "keyname=value" pair in your setup string must be terminated with a semicolon.

"key=value;key2=value1,value2;"

If you want a literal comma or a literal semicolon inside one of your fields you must type the following:

^, A literal comma.
^; A literal semicolon.

Each object class documents the keynames and the parameters it

expects to see immediately following. Note that all parameters have safe defaults. It is never required to pass setup parameters to an object. We recommend that you assign a unique OBJECTID to all objects you create. Later in this document we will provide a list of valid keynames and keyvalues for each object class.

Once you have defined an object, you will need to specify an **Action** in order to create it. The allowed actions are:

Fail	No object will be created if an object with the given OBJECTID already exists. The Object Editor and SysCreateObject action code is 'F'
Replace	If an object with the given OBJECTID exists, Delete the existing object and create a new object. The Object Editor and SysCreateObject action code is 'R'
Update	If an object with the given OBJECTID exists, Update its settings with the new information in the setup string. The Object Editor and SysCreateObject action code is 'U'.

You create objects on a OS/2 desktop by using the REXX function (SysCreateObject), the OS/2 function (WinCreateObject), or The Secure Workplace Object Editor. Each of these facilities recognize the **Classname, Title, Location, Setup** string, and **Action** items we just discussed. For an example lets define the REXX interface.

SysCreateObject has the following syntax:

result = SysCreateObject(*classname*, *title*, *location* [,*setup*] [,*Action*])

Result is the return value. The possible return values are 1 (TRUE) if the object was created and 0 (FALSE) if the object was not created.

The following example illustrates the use of SysCreateObject to create a Folder.

```
/*
** Sample Object Creation program OBJCREATE.CMD */
'@echo off'
call RxFuncAdd `SysLoadFuncs','RexxUtil','SysLoadFuncs'
call SysLoadFuncs
ret = SysCreateObject( `WPFolder',
       `System Administration',
       `<WP_DESKTOP>',
       `OBJECTID=<SWS_SYSADM>;', 'R')

return(0)
```

Here is the same object description in an Object Make file used by the Object Editor.

```
*
* 3 Comment lines
*
CLASS    "WPFolder"
TITLE    "System Administration"
LOCATION "<WP_DESKTOP>"
SETUP    "OBJECTID=<SWS_SYSADM>;"
ACTION   R
```

Notes.

The first line of any REXX procedure must be a comment enclosed in /* ... */brackets. It is the presence of this comment that tells the OS/2 command processor that this is to be interpreted as a REXX procedure rather than as an OS/2 batch file.

The two calls that follow the 'echo off' statement load the RexxUtil package. This package contains functions that will be needed to access the workplace shell, including SysCreateObject.

When creating objects you should include an OBJECTID definition in the setup string. The OBJECTID gives you a method to uniquely identify and operate on the object in the future. You cannot update or delete an object with the Object Editor or with the REXX functions unless you know it's OBJECTID. You can also use the OBJECTID of folder objects as a location for insertion of other objects into the folder.

Updating Workplace Objects

Perhaps the easiest way to update a workplace object's settings is through its settings notebook. While this method is convenient, it does not provide the hands-off capability required for unattended customization.

To update an object in an unattended mode you must identify it with a **name** and define the modifications parameters with a **setup** string.

Name

Is the object name. This can be specified as an OBJECTID (for example <WP_DESKTOP>) or as a fully specified file name. This parameter is the same as the location parameter described for creating workplace objects.

Setup

Is a setup string as described for creating workplace objects

You update workplace objects by using the REXX function SysSetObjectData, the OS/2 API function WinSetObjectData, or The Secure Workplace Object Editor. For an example lets define the REXX interface.

The SysSetObjectData function syntax is:

result = SysSetObjectData(*name*, *setup*)

result is the return value. The possible values are 1 (TRUE) if the object was updated and 0 (FALSE) if the object was not updated.

Each parameter has a parallel in the WinSetObjectData API and the Object Editor.

Notes:

The object update function can be used to open an instance of an object by using a setup string with "OPEN=DEFAULT;" included.

See the description of **Location** and **Setup** in the previous section for an explanation of the parameters. You can get a list of available workplace locations from the Object Editor location list.

Deleting Workplace Objects

Perhaps the easiest way to delete a workplace object is to drop it on the shredder. While this method is convenient, it does not provide the hands-off capability required for unattended customization. The shredder cannot delete objects that have their NODELETE style set. (ie.NODELETE=YES;) while the Object Manager makes short work of such objects.

You delete objects in an unattended mode by by using the REXX function (SysDestroyObject), the OS/2 function (WinDestroyObject), or the Object Editor. To delete an object you must know it's OBJECTID and its NODELETE style must be reset (ie. NODELETE=NO;)

The Object Editor action code for object deletion is 'D'. To insure that an object can be deleted you should first update its NODELETE style to (NODELETE=NO). Folder objects can be particularly hairy because they cannot be deleted if they contain objects that have the NODELETE style set.

Standard Setup Keywords

The following table shows the **"keyname=value"** pairs supported by all classes. Use these keywords in your setup strings.

KEYNAME	VALUE	DESCRIPTION
OBJECTID	<name>	This sets the object's identity. The object id will stay with the object even if it is moved or renamed. An object id is any unique string preceded with a '<' and terminated with a '>'. This may also be a real name specified as a fully qualified path name.
OPEN	DEFAULT	Opens the default view when SysSetObjectData is called.
	SETTINGS	Opens the settings view when SysSetObjectData is called.
MINWIN	HIDE	Views of this object will hide when their minimize button is selected.
	VIEWER	Views of this object will minimize to the minimized window viewer when their minimize button is selected.
	DESKTOP	Views of this object will minimize to the Desktop when their minimize button is selected.
VIEWBUTTON	HIDE	Views of this object will have a hide button as opposed to a minimize button.
	MINIMIZE	Views of this object will have a minimize button as opposed to a hide button.
CCVIEW	YES	New views of this object will be created every time the user selects open.
	NO	Open views of this object will resurface when the user selects open.
	DEFAULT	The default value of the concurrent view setting of the system will be used when the user selects open.
ICONFILE	filename	This sets the object's icon.
ICONRESOURCE	id,module	This sets the object's icon. 'id' is the identity of an icon resource in the 'module' dynamic link library (DLL).

ICONPOS	x,y	This sets the object's initial icon position. The x and y values represent the position in the object's folder in percentage coordinates.
NODELETE	YES	Will not allow you to delete the object.
	NO	Resets the no delete style and allows you to delete the object.
NOCOPY	YES	Will not allow you to copy the object
	NO	Resets the no copy style and allows you to copy the object.
NOMOVE	YES	This will set the object's no move style. You cannot then move the object to another folder. A shadow will be created on a move if the NOSHADOW style is not set.
	NO	Resets the no move style.
NODRAG	YES	Will not allow you to drag the object.
	NO	This resets the object's no drag style.
NODROP	YES	Will prevent you from dropping another object onto the object.
	NO	Allows you to drop another onto the object.
NOSHADOW	YES	Will not allow you to create a shadow link.
	NO	Resets the no shadow property and allows you to create shadows.
NOLINK	YES/NO	NOLINK is a synonym for NOSHADOW.
NOSETTINGS	YES	removes the OPEN SETTINGS item from the popup menu.
	NO	allows the OPEN SETTINGS item in the popup menu.
NORENAME	YES	Will not allow you to rename and object. Use this property to prevent a user from changing an object's title.
	NO	Resets the no rename style.
NOPRINT	YES	Will not allow you to print the object.
	NO	Resets the no print style.
NOTVISIBLE	YES	The object will not be displayed
	NO	Makes the object visible.
HELPPANEL	id	This sets the object's default help panel.

HELPLIBRARY	filename	This sets the help library.
TITLE	Title	This sets the objects title.
TEMPLATE	YES	Creates the object as a template.
	NO	Resets the object's template style.
DEFAULTVIEW	SETTINGS	Sets the default open view to the settings view.
	id	Sets the default open view to the id (0-9). Each object class will register views that use one or more of these.
	DEFAULT	Sets the default view to the default view defined by the object class.

Folder Setup Keywords

The following table shows the **"keyname=value;"** pairs supported by all Folder classes. These classes include the standard folder class WPFolder, as well as the desktop class. Use these setup strings in addition to the Standard Setup keynames.

KEYNAME	VALUE	DESCRIPTION
OPEN	DEFAULT	Opens the default view when SysSetObjectData is called.
	SETTINGS	Open the settings view when SysSetObjectData is called.
	ICON	Open icon view when object is created.
	TREE	Open tree view when object is created.
	DETAILS	Open details view when object is created.
ALWAYSSORT	YES	Sort order is always maintained. Opening and adding an object to a folder may take longer if the sort order is being maintained.
	NO	Sort order is not maintained. This is the default value.
ICONVIEW	s1[,s2,...sn]	Set icon view to specified style(s). s1[,s2,...sn] are one or more styles.
TREEVIEW	s1[,s2,...sn]	Set tree view to specified style(s). s1[,s2,...sn] are one or more styles.
DETAILSVIEW	s1[,s2,...sn]	Set details view to specified style(s). s1[,s2,...sn] are one or more styles.

(styles)	FLOWED	flowed list items in an icon view
	NONFLOWED	non-flowed list items in an icon view
	NONGRID	non-gridded icon view
	NORMAL	normal size icons
	MINI	small icons
	INVISIBLE	no icons
	LINES	lines in tree view
	NOLINES	no lines in tree view
BACKGROUND	filename	Sets the folder background. filename is the name of a file in the \OS2\BITMAP directory.
WORKAREA	YES	Makes the folder a Workarea folder

Program Setup Keywords

The following table shows the "keyname=value" pairs supported by all program class instances. These classes include the standard program class WPProgram, and the Secure Program class.

You can use these setup strings in addition to the Standard Setup Keynames when creating Program objects.

KEYNAME	VALUE	DESCRIPTION
ASSOCFILTER	filters	Sets the filename filter for files associated with this program. Multiple filters are separated by commas.
ASSOCTYPE	type	Sets the type of files associated with this program. Multiple filters are separated by commas.
EXENAME	filename	Sets the name of the program
MAXIMIZED	YES	Start program maximized
MINIMIZED	YES	Start program minimized
NOAUTOCLOSE	YES	Leaves the window open upon program termination.
	NO	Closes the window when the program terminates.
PARAMETERS	params	Sets the parameters list, which may include substitution characters

STARTUPDIR	pathname	Sets the working directory
PROGTYPE	PROG_31_ENH	Sets the session to enhanced compatibility full screen mode. (OS/2 V2.1 or later).
	PROG_31_ENHSEAMLESSVDM	Sets the session to WIN-OS/2 window in a separate session enhanced compatibility mode. (OS/2 Version 2.1 or later)
	PROG_31_ENHSEAMLESSCOMMON	Sets the session to WIN-OS/2 window in the WIN-O/S2 enhanced compatibility common session. (OS/2 Version 2.1 or later)
	FULLSCREEN	Sets the session type to OS/2 full screen
	PM	Sets the session type to PM
	SEPARATEWIN	Sets the session type to WIN-OS2 window running in a separate VDM.
	PROG_31_STD	Set the session to standard compatibility full screen mode. (OS/2 V2.1 or Later)
	PROG_31_STDSEAMLESSVDM	Sets the session to WIN-OS/2 window in a separate session standard compatibility common. (OS/2 V2.1 or Later)
	PROG_31_STDENHSEAMLESSCOMM	Sets the session to WIN-OS/2 window in the WIN-O/S2 standard compatibility common session. (OS/2 V2.1 or Later)
	VDM	Sets the session type to DOS full screen.
	WIN	Sets the session type to WIN-OS2 full screen
	WINDOWABLEVIO	Sets the session type to OS/2 windowed
	WINDOWEDVDM	Sets the session type to DOS windowed
	WINDOWEDWIN	Sets the session type to WIN-OS2 windowed
SET XXX	VVV	XXX is any environment variable. VVV sets the value of the environment variable. Also used to specify DOS settings on DOS and Windows programs.

The following example shows the setup string for a program object.

```
"OBJECTID=<SWTEST_EDITPGM>;PROGTYPE=PM;
EXENAME=C:\OS2\E.EXE;STARTDIR=C:\;ICONFILE=C:\PEN.ICO;
ASSOCFILTER=*.TXT,*.DOC;NORENAME=YES;NODELETE=YES;..."
```

To specify the DOS Setting values for a program object you use "SET KEYNAME=VALUE;". To specify ON or OFF use the value 1 for ON and 0 for OFF. For example:

```
"SET DOS_FILES=45;SET DOS_HIGH=1;SET COM_HOLD=1;
 SET HW_TIMER=1;SET DOS_BREAK=0;..."
```

To add more than one DOS_DEVICE you need to separate each device with a comma. For example:

```
"SET DOS_DEVICE=C:\OS2\MDOS\ANSI.SYS,C:\OS2\MDOS\EGA.SYS;..."
```

The following list enumerates the DOS Setting keynames and values:

SET COM_HOLD=0|1
SET DOS_BACKGROUND_EXECUTION=0|1
SET DOS_BREAK=0|1
SET DOS_DEVICE=device_driver_path
SET DOS_FCBS=number
SET DOS_FCBS_KEEP=number
SET DOS_FILES=number
SET DOS_HIGH=0|1
SET DOS_LASTDRIVE=letter
SET DOS_RMSIZE=size
SET DOS_SHELL=dos_shell_path
SET DOS_STARTUP_DRIVE=letter
SET DOS_UMB=0|1
SET DOS_VERSION=program^,maj^,min^,count
SET DPMI_DOS_API=AUTO|ENABLED|DISABLED
SET DPMI_MEMORY_LIMIT=number
SET DPMI_NETWORK_BUFF_SIZE=size
SET EMS_FRAME_LOCATION=AUTO|NONE|address
SET EMS_HIGH_OS_MAP_REGION=size
SET EMS_LOW_OS_MAP_REGION=size
SET EMS_MEMORY_LIMIT=size
SET HW_NOSOUND=0|1
SET HW_ROM_TO_RAM=0|1
SET HW_TIMER=0|1
SET IDLE_SECONDS=time
SET IDLE_SENSITIVITY=time
SET KBD_ALTHOME_BYPASS=0|1
SET KBD_BUFFER_EXTEND=0|1

SET KBD_CTRL_BYPASS=NONE|ALT_ESC|CTRL_ESC
SET KBD_RATE_LOCK=0|1
SET MEM_EXCLUDE_REGIONS=region
SET MEM_INCLUDE_REGIONS=region
SET MOUSE_EXCLUSIVE_ACCESS=0|1
SET PRINT_TIMEOUT=time
SET VIDEO_FASTPASTE=0|1
SET VIDEO_MODE_RESTRICTION=NONE|CGA|MONO
SET VIDEO_ONDEMAND_MEMORY=0|1
SET VIDEO_RETRACE_EMULATION=0|1
SET VIDEO_ROM_EMULATION=0|1
SET VIDEO_SWITCH_NOTIFICATION=0|1
SET VIDEO_WINDOW_REFRESH=frequency
SET VIDEO_8514A_XGA_IOTRAP=0|1
SET XMS_HANDLES=number
SET XMS_MEMORY_LIMIT=amount
SET XMS_MINIMUM_HMA=size

Launch Pad Keywords

The following table shows the "keyname=value" pairs supported by Launchpad class instances and its descendents. These setup strings can be used in addition to the Standard Setup Keywords. The launchpad class name is **WPLaunchPad**. This class is available in OS/2 Warp Version 3, or higher. There is no limit to the number of Launchpads that may exist in the system. The system Launchpad is defined with an OBJECTID of <WP_LAUNCHPAD>.

KEYNAME	VALUE	DESCRIPTION
FPOBJECTS	OBJECTSIDs	Adds objects to the end of the Toolbar. If multiple objects exist, the objects are separated by a comma. For example: <WP_OS2WIN>,<WP_OS2EO>. OBJECTID include path and file names
DrawerObjects	number, IDs	Adds the objects to the end of the numbered Toolbar drawer. The drawer number is followed by a comma-delimited set of object IDs or path and file names. The drawer number and first object must be separated by a comma. Examples of drawer numbers: 0=Toolbar, 1=Left-most drawer, etc.

LPCLOSEDRAWER		YES The Toolbar drawers will close after an object in the drawer is opened.
	NO	The Toolbar drawers will stay open after an object in the drawer is opened.
LPACTIONSTYLE		
	TEXT	Display the action buttons as text (the default).
	OFF	Turns off the display of action buttons.
	MINI	Displays the action buttons as mini-icons.
	NORMAL	Displays the action buttons as normal (large) icons.
LPVERTICAL	YES	The Toolbar will be displayed vertically.
	NO	The Toolbar will be displayed horizontally (the default).
LPTEXT	YES	The object titles will appear on the Toolbar. This has no effect on the objects in the drawers.
	NO	The object titles will be hidden. This has no effect on the objects in the drawers.
LPDRAWERTEXT		
	YES	The object titles will appear on the objects in the drawers. This has no effect on the objects on the Toolbar.
	NO	The object titles will be hidden. This has no effect on the objects on the Toolbar.
LPSMALLICONS		
	YES	Objects are displayed using small icons.
	NO	Objects are displayed using large (normal) icons.
LPHIDECTLS	YES	The frame controls (title bar and system menu) are hidden (the default).
	NO	The frame controls are displayed.
LPFLOAT	YES	The Toolbar will float on top of all other windows.
	NO	The Toolbar will not float on top of all other windows.

Printer Setup Keywords

The following table shows the "keyname=value" pairs recognized by **WPPrinter** class instances and its descendents. These setup strings can be used in addition to the standard setup keyword to create and customize Printer objects.

KEYNAME	VALUE	DESCRIPTION
APPDEFAULT	YES	This printer object is to become the application&csq.s default printer object for printing.
	NO	This printer object is not to become the application&csq.s default printer object for printing.
DEFAULTVIEW	DETAILS	Default open view for this printer object is in details view.
	ICON	Default open view for this printer object is in icon view.
JOBDIALOGBEFOREPRINT		
	YES	The job properties dialog is displayed before printing.
	NO	The job properties dialog is not displayed before printing.
JOBPROPERTIES		filename The complete path to a binary file containing the default job properties for this printer object. This data can be obtained by using the SplQueryQueue API of the spooler.
OUTPUTTOFILE		
	YES	The output of this printer object goes to a file. The user will be prompted for a filename each time a print job is submitted to this printer object.
	NO	The output of this printer object does not go to a file.
PORTNAME	portname	The names of already installed ports to which this printer object is to be attached. In the case of more than one port, specify a comma-separated list.

PRINTDRIVER	driver.device	The complete name of the print-driver that this printer object is to use. For example: 'LASERJET.HP Laserjet IIP'. In the case of more than one printdriver, specify a comma-separated list. These printer drivers must already be installed. The printer-driver name is the title of the driver icon in the Printer Driver page of the Printer device settings notebook.
PRINTERSPECIFICFORMAT		
	YES	The printer object spools print jobs in PM_Q_RAW format.
	NO	The printer object spools print jobs in PM_Q_STANDARD format.
PRINTWHILESPOOLING		
	YES	The printing is enabled while the job is spooling.
	NO	The printing is disabled while the job is spooling.
QSTARTTIME	time	The time when the printer object starts printing. The time format is HH:MM, and the base is a 24-hour clock.
QSTOPTIME	time	The time when the printer object is to stop printing. The time format is HH:MM, and the base is a 24-hour clock.
QUEUENAME	name	The local queue name for the printer object. If a queue name is not specified, one is created by the printer object. The QUEUENAME key will be ignored if this object has already been assigned a queue.
QUEUEDRIVER	qdrvname	The queue driver name. The queue driver must already be installed.
SEPARATORFILE		
	filename	A separator file that prints before each print job.

Network Printer Setup Keywords

The following table shows the "keyname=value" pairs recognized by the **WPRPrinter** class and its descendents. These setup strings can be used in addition to the Standard Setup Keywords to create and customize Network Printer objects. Remote or Network printer objects represent a print resource on another computer or server. A network must be installed before objects of this class will behave properly.

KEYNAME	VALUE	DESCRIPTION
ICON	filename	The name of the .ICO file to be used as the icon for this object.
NETID	<network>	The full name of the printer resource as it is known to the network. For example: LS:\\SERVER\LASERJET The NETID key will be ignored and FALSE will be returned if this object has already been assigned a NetId.
REFRESHINTERVAL	value	Time interval, in seconds, when the printer object is refreshed.
SHOWJOBS	ALL	All jobs are displayed in the printer object.
	OWN	Only the current user's jobs are displayed in the printer object.

Glossary of Terms

Access Control

Refers to the enforcement of user privileges. The Secure Workplace includes a Workplace access control class in the Standard Edition. In the Professional Edition a file access control class is added.

Access Control List

a list of User Privileges or Resource Privileges.

Action

Refers to an action taken upon a workplace object. Available actions are Create, Delete, or Modify. OS/2 Warp defines additional actions such as Move, and Copy.

Archive or Archive Directory

Refers to directory containing one or generations of backup desktops.

Authentication

Refers to the process by which users proves to the system that they are who they say they are by entering a password only they should know.

Classname

A workplace object class or type. The classname is a case sensitive word such as WPProgram, WPFolder, WPPrinter, and others.

Create a Desktop

A Traveling Workplace function that constructs a new desktop from resource file(s).

Backup a Desktop

A Traveling Workplace function that saves the active desktop plus additional files from a local workstation into an archive directory.

Desktop

Your interface to Workplace Objects. The Desktop is a folder

usually named (\DesktopX) where X is a alphanumeric character assigned by Traveling Workplace. The Desktop can have any name and can reside on any drive. The desktop also consists of a user profile (ie.OS2.INI) and a system profile (ie.OS2SYS.INI). The desktop folder is always open when the Workplace shell is active. The Desktop Object ID is usually <WP_DESKTOP>. Workplace is a synonym for Desktop.

Desktop Management

The control, protection, and administration of Desktops, Workplaces, and/or workstations. Desktop management activities can include Backup, Restore, Create, Switch, Configuration, Access Control, Privilege assignment, and Software Distribution.

Desktop Resource File

Refers to a User Resource File that was made from INI.RC. Traveling workplace will build a desktop from a User Resource file. Object Editor can Read and Write Resource Files.

Dynamic Password

A password that is based on the system clock and a seed string you assign.

Enterprise License

A site, network, or multiple station license.

Folder

A directory object in your Workplace. Folder objects usually appear as icons that look like file folders you can purchase at a stationay store.

Identification

Refers to the part of the sign on process where users enters their user ID.

Location

For object creation this refers to an object's containing folder. For object deletion and modification this refers to the object itself.

Object
Usually refers to a Workplace Object.

OBJECTID
A unique name that can be used to refer to Workplace Object. You can also specify a fully qualified file system path. An OBJECTID begins with '<' and ends with '>'.

On-line Workplace
A Desktop that resides on a local machine and is not in an archive directory. On-line workplaces can be active or inactive. Only one desktop can be active at a time.

Parent or Parent Folder
Refers to the folder or directory that contains an object you are interested in.

Privilege
Refers to a users access level to an object. Privileges include open, execute, read, write, delete, copy, move, rename, shadow, settings, visible, drag, drop, as well as pop-up menu items.

Profile
Usually refers to a file containing Applications, Keys, and KeyValues examples are OS2.INI and OS2SYS.INI.

Remote
Parlance for resources residing on Network Server, Local Area Network, Wide Area Network. Also used to refer to administration of off-site workstations.

Restoring a Desktop
A Traveling Workplace function that copies a desktop plus additional files from an archive directory into the local workstation. The restored desktop becomes an on-line desktop. The restored desktop becomes active after it is restored.

Resource
A local or remote object. Also refers to printer and communications ports. The Secure Workplace cannot enforce access to a remote machine that does not have the product

installed. Port access control is possible in the professional edition with the file access control driver installed.

Resource Privilege

The list of objects or resources and their privileges that has been granted to a user. The Secure Workplace constructs these privileges when the user signs on.

Secure Workplace

The name of Syntegration's Security and Desktop Management product.

Setup string

A series of "keyname=value" pairs, that defines the behavior of a Workplace object. this is also known as assigning settings.

Settings

The properties of an object. You can change an object's settings with a setup string or through it's settings notebook.

Settings Notebook

The user interface to an object's settings. You can open up the settings notebook by placing the mouse over the object icon, pressing the right mouse button, and selecting the "Settings" pop-up menu option. In OS/2 V2.XX the setting option is in the "Open" cascaded menu.

Sign OFF

Synonym for logout or logoff. The reverse of sign on. After Sign OFF the user is no longer privileged. A Sign ON or Shutdown follows.

Sign ON

Synonym for login or logon. The procedure by which users identify and authenticate themselves by entering a User ID and a password. Sign ON can be local or remote. remote signon is the same as single sign on.

Single Sign-ON

Synonym for login or logon. The procedure by which users identify and authenticate themselves by entering a User ID and

a password. The user is usually authenticated by a Network Server, Remote Host, and/or another user registry residing on the local machine. The Secure Workplace uses this feature to allows administrators to maintain a centralized password database, or to allow for sign-on to multiple hosts.

Switching Desktops

A Traveling workplace function that lets you change the active desktop. You switch between on-line desktops.

System Profile

Refers to a Profile that the OS/2 Operating system uses to store system information The file name is usually OS2SYS.INI.

System Resource File

Refers to a Resource File that can be converted to a System Profile. You use the MAKEINI.EXE utility to perform the conversion. OS/2 comes with a default System Resource file named INISYS.RC.

Traveling Workplace

The name of Syntegration's Desktop Image management product. This program is included with The Secure Workplace Professional Edition.

Title

Usually refers to an object's title. This title appears below the object's icon

Unattended Mode

An environment where a program executes without user or administrator attention or interference.

Unattended Installation

Installing a product on a local workstation without user interference or administrator attention.

Unattended Customization

Product configuration on a local workstation without user interference or administrator attention.

User

The person who signs on to a workstation.

User Privilege

An object or resources access control list. The list consists of users and there privileges to a resource. The system administrator grants user privileges.

User Profile

Refers to a Profile that the OS/2 Operating system uses to store information about your desktop. The File name is usually OS2.INI. Application programs also use this file to store persistent information that can be recovered after reboots.

User Resource File

Refers to a Resource File that can be converted to a User Profile. You use the MAKEINI.EXE utility to perform the conversion. OS/2 comes with a default User Resource file named INI.RC. User Resource files can be used build new desktops. Traveling workplace will build a desktop from a user resource file. Object Editor can Read and Write Resource Files.

Workplace

Synonmy for an OS/2 desktop. Also used as a short hand name for the Workplace Shell. You can also extend this to refer to all the objects that exist on your hard drive(s).

Workplace Object

Any icon you can see on a OS/2 Desktop. These objects have other properties you can set from their settings notebook. Files and Directories are workplace objects. Abstract objects are located in the Desktop' User Profile (ie.OS2X.INI).

Workstation

A personal computer.