Secure4Access (GUARDIAN)

A Technical White Paper

NOTICE

As Secure4Access is a software product which is subject to change, S4Software, Inc. reserves the right to make changes in the specifications and other information contained in this document, without prior notice. While S4Software, Inc. has made every effort to ensure the accuracy and completeness of this document, S4Software, Inc. cannot be held liable for any errors or omissions. No information contained in this document shall be deemed to be a warranty for any purpose whatsoever.

RESTRICTED RIGHTS LEGEND

Use, duplication or disclosure by the Government is subject to restrictions as set forth in subprogram (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at subparagraph DFARS 252.227-7013.

S4Software, Inc.
6633 Convoy Ct.
San Diego, CA 92111

Phone: 858-560-8112
Fax: 858-560-8114

E-mail: sales@s4software.com
URL: www.s4software.com

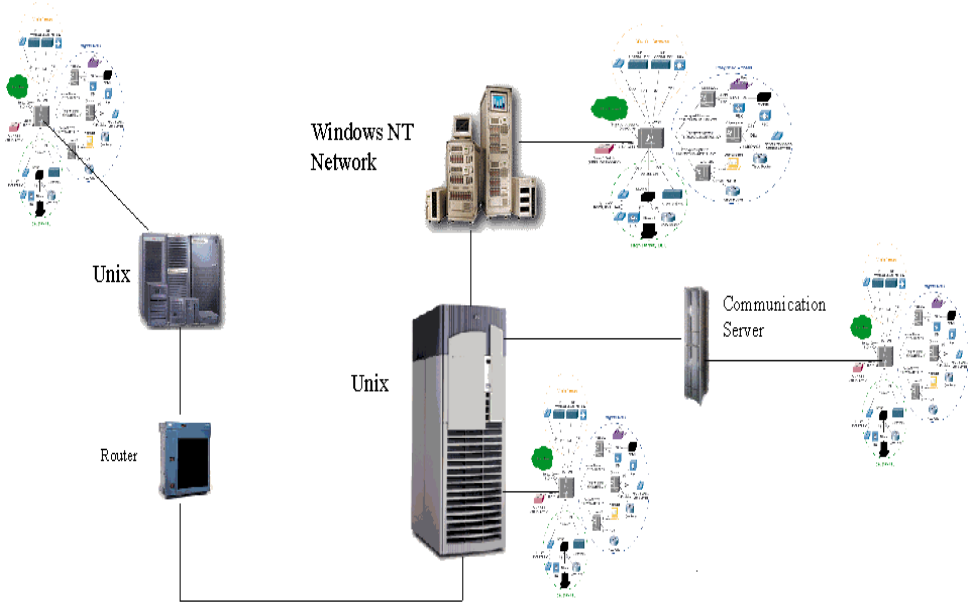
Table Of Contents

The Issue

Account access control and system administration are central components of a robust security policy. Implementing strong controls which at the same time enhance user productivity remains a challenge. Industry-wide we find:

- 60% of all calls to the help desk are password related.
- Scarce technical resources are diverted to mundane system administration tasks which can be automated.
- Multi-host, heterogeneous operating system environments introduce complexity and increase the potential for security vulnerabilities.
- Limited audit facilities make preemptive detection and resolution of problems difficult.

Tools for resolving such issues differ widely among Unix platforms and are often intelligible only to very knowledgeable Unix system programmers. By themselves, most versions of Unix have very limited access control capabilities. Devising and maintaining a comprehensive account access policy is even more complicated in a heterogeneous Unix and Windows™ environment with limited, non-overlapping access control features.



The Solution - Introduction to Secure4Access

Secure4Access solves account access and administration problems by providing a rich set of access control features and a common, easy-to-use interface for most major versions of Unix and Windows:

- Administer accounts on one Unix server for an entire network of heterogeneous Unix and Windows systems from the central Secure4Access administration host.

- Depend upon the Distribution Manager option to automatically store and forward updates to all designated systems.

Secure4Access is a set of programs designed to implement a sophisticated access control policy. It includes:

- An administration interface (character, Motif, and command line based versions) used to build and maintain user accounts on one or many systems at the same time.

- A program which runs during the login process and a daemon which together monitor and control all logins.

- Unix daemons and the Secure4Access ageNT which receive and process password change and account creation, edit and deletion requests on remote hosts including NIS/NIS+ servers, stand-alone Unix servers and Windows.

- The optional Distribution Manager is intended for sites with large numbers of hosts to manage. It provides a completely redundant multi-level distribution system which manages account propagation.

- Site-maintainable dictionaries giving valid and invalid passwords for use in password generation and validation as well as options for enforcing FIPS-181, DoE, and DoD password formats

The Secure4Access system provides additional layers of security over the standard Unix environment by automatically trapping all user login attempts in order to enforce additional validation checks. As the normal Unix login system only allows user identification and limited password aging, Secure4Access gives the system manager a method of extending access control and thereby enhancing the security of the system. Secure4Access access controls include defining how, where, and at what time the user is allowed to access the system. In addition, the manager can control allocation of system resources to each user, and can limit the number of concurrent sessions per user.

Summary

Secure4Access supplies a network-wide framework for establishing, maintaining and enforcing your password and user account security policy.

Secure4Access enhances security and simplifies account administration without kernel modification.

Secure4Access implements industry best-practices standards including synchronized, network-wide account names, UIDs and GIDs.

Secure4Access introduces hierarchical system management privileges.

Secure4Access provides a rich set of facilities that allow you to audit and report upon your system(s) integrity.

Secure4Access comes with industry-standard defaults, and with more than one hundred tailoring options.

Secure4Access allows simple integration with existing applications via command line or API.

Secure4Access is developed, supported and maintained by a company dedicated to software excellence!

Features

- Provides easy-to-use menu and Motif-based GUI programs with automatic help messages for the creation and maintenance of user accounts.
- Offers creation, editing, locking and deletion of accounts on one system or many with a single operation.
- Simplifies account creation by offering site-editable account templates.
- Partitions the Unix ‘all or nothing’ root privilege by defining additional '*Security manage*r' and '*Network manager*' privileges for executing the Secure4Access menu programs and updating accounts on remote hosts or domains.
- Defines a ’*Password manager*’ privilege so the non-root help desk operator can change the password of non-privileged accounts.
- Permits Secure4Access management privileges to be partitioned by role, including restricting privileges which can be assigned to accounts.
- Ensures account names, UIDs and GIDs are synchronized across multiple platforms.
- Defines an expiration date for an account after which logins will be denied.
- Requires that users change their passwords on a regular basis by specifying a minimum and maximum life for the password. Single use passwords can also be specified which must be changed on the first login or on every login.
- Generates random passwords consisting of one or two words from a site-editable dictionary, by using the FIPS-181 password algorithm, the DOE password standard, or the DoD password standard. The passwords may include randomly selected integer and punctuation characters.

- Validates passwords according to an account-specific template. Passwords are also checked to be sure that they are not easily predictable, are not contained in a site-editable dictionary of illegal passwords, and that old choices are not reused. Secure4Access keeps a history of the last 20 passwords.

- Automatically inactivates accounts after too many invalid password entries.

- Automatically updates user password changes across multiple hosts, NIS domains, NIS+ based networks and Windows networks (with Secure4Access ageNT). Users do not have to worry about whether the account is on the local system or in the global NIS maps, the same password changing interface is used regardless of the account type.

- Invokes a user-defined alarm script when a potential security violation is detected.

- Restricts particular accounts from being accessed from specified terminals, the system console, over a network, from specified hosts, on modem lines, or via `ftp`, 'r' commands, and `su`. Also restricts logins to specified hosts even when the account is global.

- Specifies which users are permitted to `su` to a particular account.

- Specifies the time windows during which a user is permitted to log in. Users can be optionally forced off the system when their time window closes.

- Allows additional 'private' comments to be stored in the user's Secure4Access Profile, available only to the system administrator.

- Locks or terminates sessions when they have become inactive.

- Permits the user to explicitly lock an X session when they leave their terminal.

- Permits role-based system administration. Users can be assigned to a role (Secure4Access login group), default privileges inherited from the role’s account template, and system access can be restricted by role (including the maximum concurrent logins allowed).

- Limits the number of concurrent login sessions that the user is allowed.
- Logs all account access by time and location.
- Offers a 'wrapper' for the `ftp` daemon so that `ftp` access to accounts can be restricted and logged.
- Keeps redundant copies of Secure4Access files on any NIS slave server and provides automatic failover in the event that the master server becomes unavailable.
- Maintains the `/etc/group` file and NIS group map so that users can be added to and removed from supplementary access groups.
- Provides a complete set of reports detailing the various accounts on the system according to user-defined criteria. The report types are shown later in this document.
- Offers an extensive array of utilities and a command line interface for batch processing which aids in monitoring and maintaining the system login environment.
- Offers an API for additional site-specific security checks.
- Provides extensive tailoring options including user-defined scripts.

NOTE: Most features are site-configurable but are supplied with industry 'best practice' defaults.

Secure4Access enhances UNIX

	Secure4Access	IBM - AIX	DG/UX (88K, Intel)	DIGITAL UNIX	ICL-DRS/NX	DYNIX/ptx	HP/UX 10	LINUX	SGI-IRIX	NCR-SVR4	SCO RELEASE 5	SIEMENS-SINIX	SOLARIS 2	SunOS	Unisys SVR4
Cross domain account administration	X														
Assign users to login group & control number of logins per grp	X														
Restrict users from changing account password	X							M							
Set minimum and maximum password life	X				X	X	X	X	O	X	X	X	X		X
Assign minimum password length	X	X		O	P		P	M		P	P	P	P		P
Define password input format	X	X						M			X				
Allow up to 15 character password	X														
Allow/Disallow users to choose own password	X			O			O				X				
Maintain password history	X	X		O				M							
Auto password generation w/option FIPS-181	X			O			O	M			X				
Maintain valid and invalid password dictionaries	X	X						M			X				
Single use passwords	X							M							
Assign account expiration date	X	X			X	X	O	X	O	X	X	X	X		X
Set group password	X														
Inactivate (lock) accounts	X	X		O	X		O	X	X	X	X	X	X		X
Allow users to manually lock session	X														
Force users to change password	X			X		X									
Allow/Disallow console login	X														
Allow/Disallow modem login	X		X		X		X			X	X	X	X		X
Allow/Disallow network login	X	X													
Allow/Disallow access via ‘su’	X	X						M							
Specify which accounts may ‘su’ to a particular account	X							M							
Allow/Disallow access via ‘r’ commands	X	X						M							
Allow/Disallow access via ‘ftp’	X	P	P	P	P	P	P	X	P	P	P	P	P	P	P
Set login time windows	X	X		O											
Set maximum login time per day	X														
Allow/Disallow batch jobs outside of login time	X														
Inactivity lock/logoff	X														
Set home filesystem disk quota	X	P	P				P		P				P	P	
Allow/Disallow logins to or from specific hosts	X							M							
Restrict specific ports	X	X													
Automatically run alarm script on exception	X														
Generate reports - User selected criteria	X														
Generate reports - Special security consideration	X														
Generate reports - Account/user activity	X														
Inactivate expired accounts (one step utility)	X														
Batch account editor	X														
Auto account inactivation after too many bad login attempts	X	X		O			O	M	X						
Auto account inactivation if unused for user-defined time	X				X		O	M	O	X			X		X
Command interface	X	X			X		X	X		X	X		X		X
Run user defined script - account setup, pwd validation, etc.	X														
API	X														
Set maximum concurrent logins	X														
Partition security privileges	X														

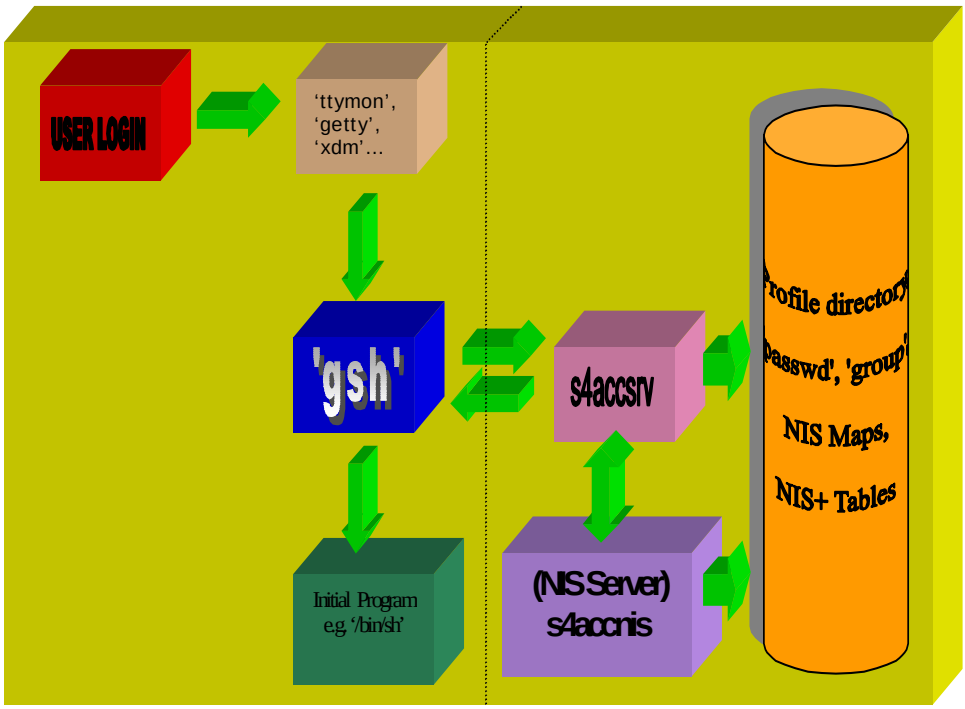
This table refers to mechanisms within the operation system and administrative utilities which do not require additional products, custom modifications or programming
M = Available if appropriate PAM modules are created and installed
O = Optional (Requires system configuration change to enable shadow, password adjunct or protected password files.)

Architecture

Major features of Secure4Access are explained briefly here. First is Secure4Access's ability to enhance system security without modifying the Unix kernel. Secure4Access's central administration and Distribution Manager capabilities are also discussed.

Access Control

Secure4Access assumes control of the login process after the system login process (ttymon or xdm) completes. This system login process starts the initial program specified in the system password file, normally a standard shell. For a Secure4Access-controlled account, this initial program is the Secure4Access user program, `gsh`. As this is the first program run, Secure4Access is able to trap the login before the user gains control. The `gsh` process examines its environment to determine what is occurring (local or remote login, a remote shell request or the `su` and `newgrp` programs), then communicates with the Secure4Access server daemon (`s4accsrv`). This daemon process retrieves the Secure4Access profile for the user (either from a local filesystem, NIS master or slave). This file, which is unique to each user, contains information describing the user's access privileges and is used to validate the access attempt.



After the daemon has determined whether the user's access attempt is valid, it returns a message to `gsh` giving all the necessary information to either complete or terminate the access. If the access is successful, `s4accusr` will fork a process running the user's normal login program, otherwise it displays the appropriate error messages and then terminates the access attempt. A wrapper for the ftp daemon is also supplied which permits ftp accesses to be authenticated in the same way.

If the daemon determines that the user's password has expired, it examines the profile to see if the user is permitted to choose their password. If not, then a new password is generated for the user, otherwise it notifies `gsh` to request a new selection which is then passed back to the daemon for validation. In either case, the new password is stored in the user profile and system files (if specified). The old password will be added to the user's password history to ensure that it is not repeated for up to 20 future selections. If the account is contained within NIS/NIS+ then the 'passwd' map/table will also be rebuilt.

In addition to normal and remote logins, some programs such as `su` and `newgrp` execute the initial program as given in the `/etc/passwd` file, i.e. `gsh`. When it is executed, it determines the nature of the invocation such that it can perform all necessary checks. In the case of `su`, the access is monitored to ensure that it is permitted for this account, and if so, whether the requesting user is in the list of accounts permitted to `su` to this account.

For those systems which are part of an NIS (`yp`) or NIS+ domain, Secure4Access will automatically interface with and maintain the various NIS maps or NIS+ tables. In environments that require assured system access even if the master server is unavailable, Secure4Access can keep a redundant set of all account information on a designated slave server(s). This information is always kept current and available for use. Secure4Access also allows for assured password changes when the master is down, unlike `yppasswd` that can only communicate with the master server.

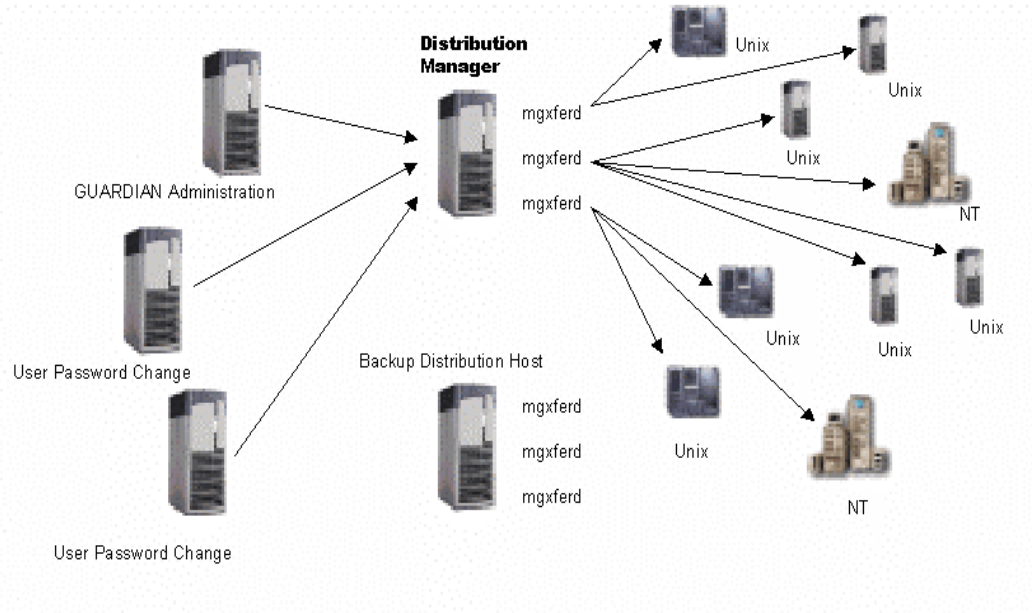
Central Administration

The Secure4Access package can be configured to offer the convenience expected from an NIS global account without introducing the insecurity associated with NIS. To accomplish this, Secure4Access maintains identical accounts for a user on each system that user is permitted to access. Secure4Access does this automatically by propagating account information to remote hosts including Windows hosts whenever there is a change. This includes account creation, deletion, rename, inactivation, activation, privilege changes and password changes. Unlike a global NIS account which by default permits access to any host in the domain, only the hosts a particular user is permitted to access receive updates. Secure4Access therefore makes it possible to administer an entire network of heterogeneous Unix hosts and Windows hosts from a single, central location. It also insures that when the user changes their password on one Unix system, all their account passwords will be updated.

Secure4Access accomplishes this through the use of a daemon or a windows service which runs on each host which will receive updates. The daemon or service 'understands' the environment in which it is running: the operating system type, whether it is an NIS or NIS+ master server for a domain, a PDC, etc. The daemon performs whatever steps are necessary to apply the changes. Thus the user perceives they have a single username, password and access privileges on all systems they access. Secure4Access achieves this by transferring a small binary message to each host. It thus avoids problems which plague NIS, including time-consuming rebuilding and pushing of the password map each time a user changes a password, the insecurity of publicly readable encrypted passwords via `ypcat`, etc.

Distribution Manager

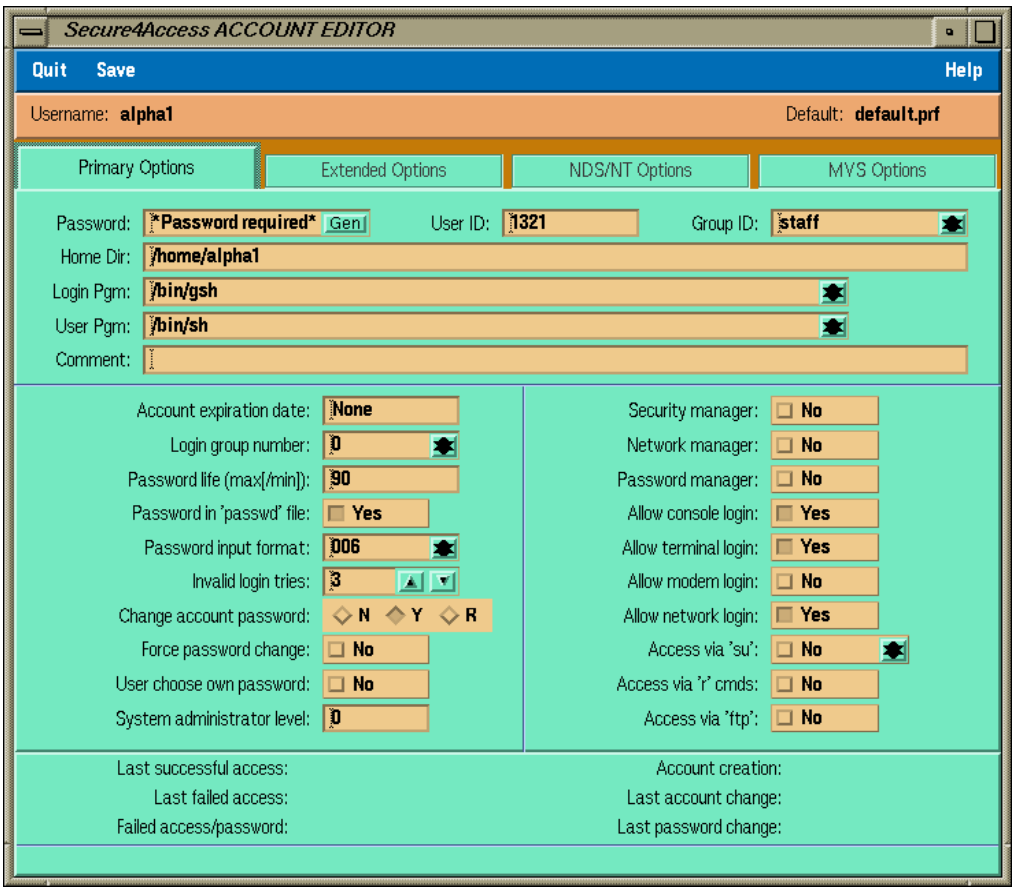
While Secure4Access offers the capability to propagate account information to remote hosts, in larger networks the Distribution Manager option is recommended. This option provides a separate daemon which manages multiple concurrent file transfer daemons (`s4dmxfer`). It is fully redundant, to insure a central distribution host is always available. It provides for queuing and retransmitting of messages on error.



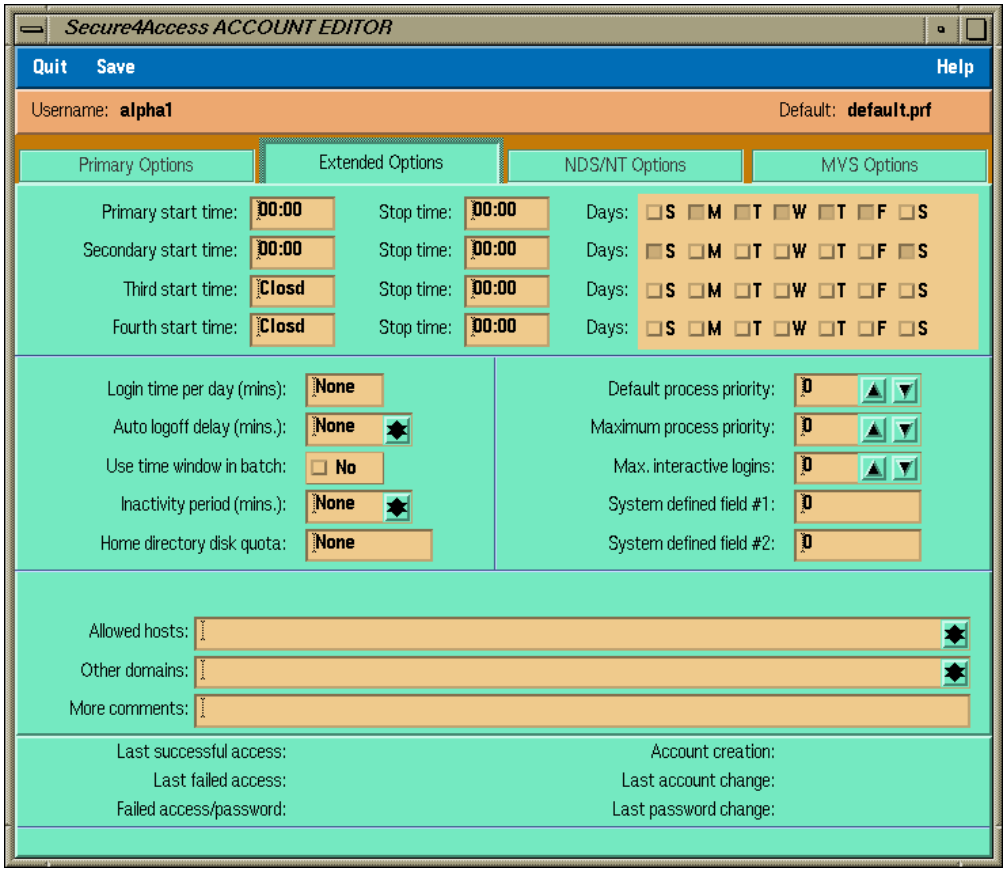
The Secure4Access Profile

The Secure4Access menu program includes an easy-to-use program for creating and editing user accounts. The primary display includes the system 'passwd' fields, along with the fields which define password control and system access locations. The extended options screen contains user access time windows and other system usage privileges. Each of the fields is described on the pages following the Option Screens. Only the upper portion of the primary options display is significant for non-Secure4Access accounts.

Primary Options Screen



Extended Options Screen



Specifics

System 'passwd' fields: upper portion of the Primary Options display

These are standard Unix 'passwd' fields, except that when *Login Pgm* is set to `/bin/gsh`, the *User Pgm* field will contain the user's normal start-up shell, e.g. `/bin/sh`. The same username and password will be used if a Windows account is to be created.

Account expiration date

Logins to this account will be refused after this date. The account will be inactivated.

Login group

The login group (role) is intended to segregate users by function, and can be used to limit the maximum number of concurrent sessions for any set of users. Activity reports can also be generated by login group.

Password characteristics: password life, storage location and format

The *Password life* field is used to set the minimum and maximum life for a password. If the maximum life is negative, then the user will be forced to change the password during the next login session. If the password is kept only in the Secure4Access profile, then the password length can be up to 15 characters. Password format controls include the minimum number of numeric or punctuation characters, maximum repeats of a character, and minimum length.

Invalid login tries

Defines the number of consecutive invalid login attempts allowed before the account will be inactivated.

Password updating: change password, force password change and user choose password

These fields define how the password is updated. By default, a user can change their password but must accept a system-generated selection. If *Force password change*=**`N`**, password updating is done by running a shell command, otherwise it occurs automatically during the user login. The **`R`** option allows password changes to update accounts in remote domains including other hosts, NIS/NIS+ domains, and Windows domains.

System administrator level

This field is for use with the Secure4Privilege package. Secure4Privilege can be used to control access to system programs or scripts. Among its many features, Secure4Privilege allows programs that normally require `root` privileges to be run by users without knowledge of the root password if those users have the appropriate system administrator level.

Manager privileges

Defines the management privileges for this account. *Security manager* is required to run the Secure4Access menu programs. *Network manager* is needed for cross-domain updates. *Password manager* permits the non-root operator to change another user's password using the `s4accpwd` utility.

Login access modes

These fields set the locations from which this account may be accessed. These include console, terminal, modem, and network login and access via `su`, 'r' commands and `ftp`.

Time windows: login time per day, auto logoff delay and use time window in batch

These fields define time windows during which logins are allowed. The *Auto logoff dela*y field specifies the action taken when the window closes. The *Use time window in batch* field defines whether batch jobs submitted via `at` will run after the user's time window closes. Time windows can be established for Windows accounts.

Inactivity period

Defines the allowed session inactivity time, and the action taken when it becomes inactive (i.e. lock or terminate).

Home directory disk quota

If set to a non-zero value, this field will determine the maximum size of the user's home directory or disk quota (if allowed by your Unix implementation).

Process priority

These fields determine the starting and maximum process priorities allowed for this user (if allowed by your Unix implementation).

Maximum interactive logins

This field sets the maximum number of concurrent logins (domain-wide) allowed for this account.

Allowed hosts/Login hosts

Depending on the configuration setting, the hosts from which or to which logins are permitted can be specified.

Other domains

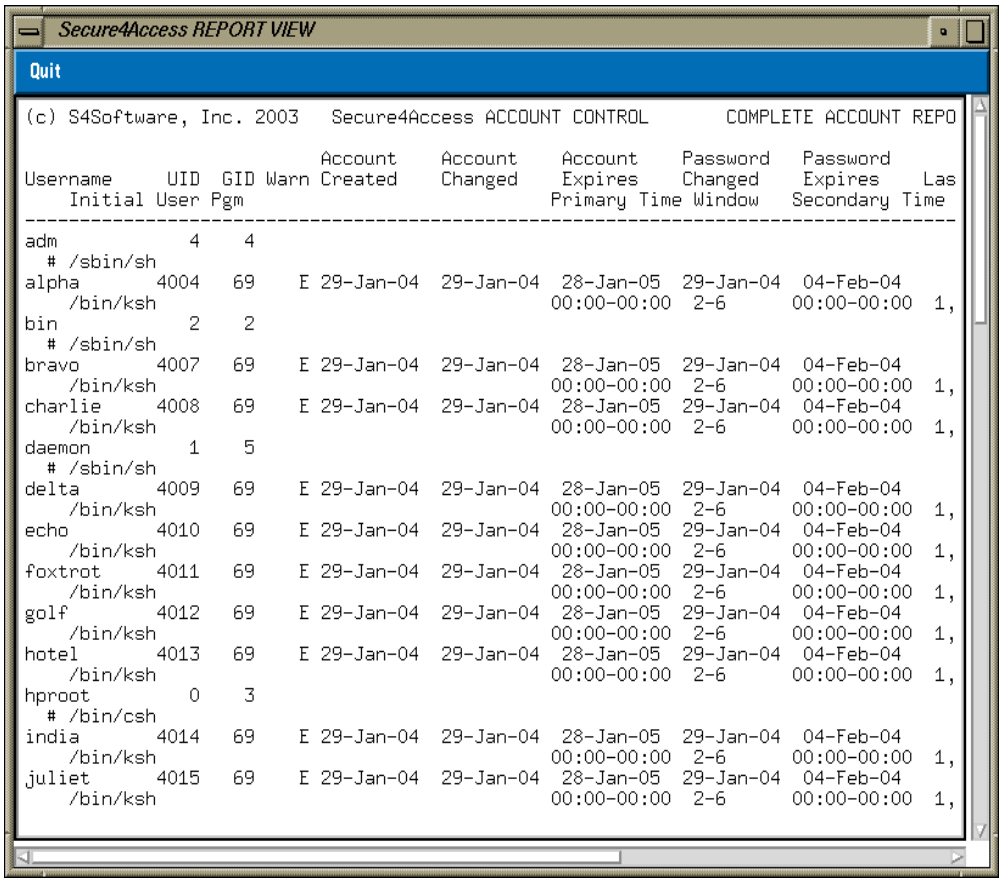
This field identifies other domains (i.e. non-NIS hosts, NIS, NIS+ and Windows domains) where the account is to be copied on account creation, edit, password change, etc.

More comments

A private comments field accessible through the API. Note that the comment field of the system password file is ‘world’ readable whereas this field is only accessible to system administrators via the menu program and API.

Report Options

The reports can be used to generate selected lists of the various accounts on the system, sorted by name, expiration date, role (login group), or UID. Shown below is a sample of the *Complete Account Report.* The facility to export comma delimited output is also offered.



Complete account report

This creates a detailed listing of all or a defined subset (by name) of the accounts on the system. The report can be printed in either normal or extended detail mode.

'Super' account report

This shows accounts having one or more of the following attributes or privileges: User ID less than 20, Group ID is 0, or any manager privilege set.

Expired passwords report

This report lists any accounts with a password that is older than the specified password life. Pre-expired accounts are listed if they are more than 7 days old.

Expired accounts report

This report shows all accounts which are past their specified profile expiration date.

Inactivated accounts report

This lists all accounts which are currently inactive, i.e. those accounts where the login permission has been turned off.

Unused accounts report

This report shows all accounts that have been unused for a given time.

Network/modem privileges report

This report lists all accounts which have modem or network login privileges, `ftp` access or have the network manager privilege.

User login group accounts report

This report lists all accounts belonging to a specified Secure4Access login group.

Password validation report

This report lists accounts for which the password fails any of the password validation criteria.

System, audit log and user activity reports

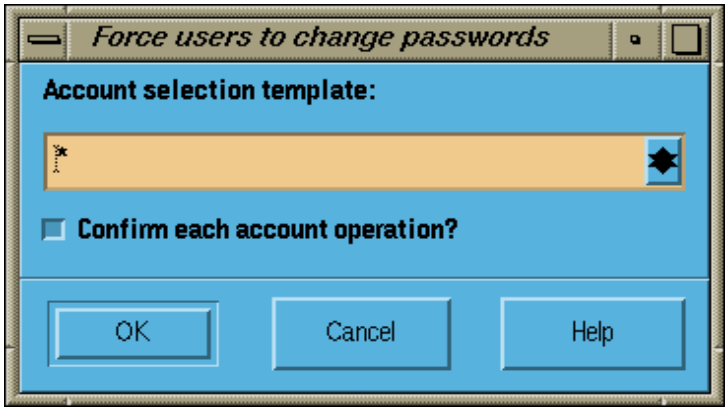
These reports show all login and logout activity by user, including date, time, PID, login location and connect time. The audit log includes Secure4Access menu program usage, daemon messages, etc.

Account exception report

This report shows accounts that represent potential security problems.

Utility Options

The utility options provide a variety of functions for maintaining and monitoring the various accounts and login activity on the system. Shown below is a sample of the *Force Users to change passwords* utility.



Install accounts into Secure4Access

This option integrates existing accounts into Secure4Access. It picks up information from the system password file, creates a Secure4Access account profile, and sets the initial program to `gsh`.

Force users to change passwords

This option is used to modify all specified accounts such that they will require a password change during the next login.

Batch account creation

This utility is used to create one or more accounts by duplicating an existing account.

Change field in multiple accounts

This option is used to modify the value of a user profile field in a set of accounts.

De-Install Accounts from Secure4Access

Allows the system administrator to easily remove any or all accounts from Secure4Access control.

Activate and inactivate user account

These options enable and disable logins. Inactivating an account makes it unavailable for login without the necessity of deleting the account or modifying the password.

Inactivate expired accounts and passwords

These functions will inactivate all accounts where either the account or its password is past the specified expiration date.

Inactivate unused accounts

This utility examines all accounts and inactivates those that have not been used for a user-specified number of days.

Remove inactivated accounts

This option deletes all accounts that have been inactivated

Edit Unix and login groups

This option is for maintaining the Unix group file, map or table and the Secure4Access login groups cross-reference file. It can be used to list, create and delete Unix groups, and to add or remove users from those groups.

Manage the netgroup file

This option permits maintenance of the Unix netgroup file.

Password dictionaries maintenance

This menu is used to maintain the password dictionaries. The valid word dictionary is used for generating passwords. The invalid word dictionary is for validating user-supplied passwords.

Audit Trails

The ability to create a detailed audit trail of all normal and exceptional system activity is important. To fulfill this requirement, Secure4Access optionally keeps three logging files to track account maintenance and system access. These files are kept in the `/usr/secure4/secure4.upf` directory which requires privileged access.

The first audit file (`s4access.log`) is a text file used to record all activity relating to the creation or modification of accounts, along with recording all exceptional login attempts. This file includes information on the user identity and time of all execution requests to the main menu program. Also included is a record specifying each account creation or modification. The login exception records are kept for all users whose login is aborted because it was outside the parameters defined for the account. These include requests from disallowed ports and outside of the login time windows. In addition to these records, this file also records the date and time when the server daemon is started and stopped, and when the syslog facility is enabled or disabled.

The optional `s4access.slg` audit file contains a record for all login attempts, both valid and invalid, and all logouts, whether normal or forced. These activity records include the username, process ID number (pid), login group number, port location and time. In the case of invalid login attempts, the reason for refusing the login is also recorded. Because this information is only useful to the extent that it is possible to generate meaningful reports, a syslog analysis option is included in the main menu program. This option will generate either summary or detailed login activity reports for all users, for any specified login groups, or for a single user. The report also includes a summary of all normal and failed login attempts according to access type and total connect time.

The binary format `s4access.clg` audit file combines `s4access.slg` and `s4access.log` information. Secure4Access can produce a combined log report from the data. More importantly, this log makes all Secure4Access events visible to auditGUARD for real-time monitoring and alerts[1], and remote archiving.

1. Alerts can be generated by both Secure4Access and auditGUARD. They can be sent to a pager, e-mail, or to any number of alerting systems such as HPOpenview, Tivoli, BMC Patrol, etc.

Secure4Access ageNT

More and more companies are instituting multi-domain networks incorporating Windows™. Secure4Access ageNT comes to the rescue, simplifying the system administrator's job of maintaining accounts on diverse platforms. Now it is possible to create, edit and delete accounts on your Windows system right from your Unix 'Command Post'. No need to run from room to room!

The Windows user fields Secure4Access ageNT will update are shown below.

Username

The Secure4Access ageNT creates and maintains Windows accounts with the same username and password as the Unix account.

Password

When a user with an Windows domainname in their Secure4Access profile changes their account password it will automatically be updated in the Windows domain as well as in the Unix domain(s).

Description

This field corresponds to the *Comments* field on the Secure4Access Profile Primary Options Screen (shown on page 14).

User Cannot Change Password

This field corresponds to the *Change account password* field on the Secure4Access Profile Primary Options Screen (shown on page 14).

Account Expires

This corresponds to the *Account expiration date* field on the Secure4Access Profile Primary Options Screen (shown on page 14).

Logon Hours

This corresponds to the settings in the Primary start time and end time, and the Primary days setting in the Secure4Access Profile Extended Options Screen (shown on page 15).

Frequently Asked Questions

If I install Secure4Access on my system, will it immediately affect all my users?

Secure4Access only controls those users that you specify. To place a user under Secure4Access control you must create a Secure4Access User Profile. In the profile (as shown on page 14 and 15), the login program must be set to `gsh`. Once Unix validation is complete, it starts the login program (specified in the 'passwd' file), in this case `gsh`. At this point, Secure4Access will validate the login, and do any additional checks specified in the profile, and start the user's initial program or shell.

Am I going to need to create new accounts for all my users to bring them under Secure4Access control?

NO! Secure4Access offers two options for bringing existing accounts under Secure4Access control. On an individual basis, accounts existing in the system 'passwd' file may be modified using the *Edit a user account* option, and specifying a Secure4Access profile is to be created; or, the *Install accounts into Secure4Access* batch option may be used for one or more accounts at a time. This option will install the accounts by updating their password file record and creating a new Secure4Access profile.

Do I have to reboot after I install Secure4Access?

NO! Secure4Access can be installed on your system, without taking it down, without requiring users to log out - basically without a hassle. There is no need to reboot after you have installed Secure4Access either. Secure4Access does not modify the kernel.

How much space does Secure4Access require?

Disk space requirements vary between 15 to 25 megabytes, depending upon operating system.

Can I restrict who can `su` to my configuration control account?

YES! Secure4Access can restrict `su` on a per account basis. The Secure4Access user profile provides you with an option to specify which accounts may `su` to a particular account (see page 14). This is accomplished by setting *Access via 'su'*=**Y** and then highlighting only those accounts which will be allowed to `su` to that account. Even `root` can be restricted from performing an `su` to a Secure4Access controlled account.

I need to set up thousands of student accounts every quarter and then get rid of them. Can Secure4Access help?

YES! Secure4Access has a command line interface that can be used to automate creation of your student accounts. The account expiration date can be set so that the account becomes unavailable after the end of the term. Expired accounts can be inactivated and deleted with a couple of mouse clicks.

If the users also need Windows accounts, Secure4Access will create them at the same time, and delete them at the end of the term along with the Unix accounts!

Can my help desk change my user's passwords? They don't have 'root' privileges.

YES! Secure4Access provides a *Password manager* option. With this option set in a user's Secure4Access profile, they may change a non-privileged user's password. This option does not require `root` privileges.

My users have a tendency to walk away from their desks without logging off. I'm worried about this creating an opportunity for someone else to come along and do some damage. Can Secure4Access solve this problem?

YES! Secure4Access provides you with an option to lock or terminate a user's session if it remains inactive for the period of time defined in their user profile. Callouts to user-defined scripts can be performed at the start and end of the inactivity period and prior to termination due to inactivity. The latter can be useful for insuring that applications are terminated gracefully. A utility is also provided for user's to lock their X session manually before they leave their terminal.

Do I have to create accounts separately on my Windows and my Unix Systems?

No! Just create new accounts using Secure4Access for Unix. Make sure you specify the Windows domainname in the 'other domains' field on the Extended Options Screen, and list that domain in the Secure4Access Configuration File. Secure4Access ageNT will create that account on your Windows systems for you.

What if I just want a local Windows account? Can I still create that from my Unix System?

You betcha! When you create an account using Secure4Access for Unix you can specify whether or not it will be considered a local account or global account by placing an asterisk prior to the Windows domainname in the *Other domains* field in Secure4Access. Use of an asterisk specifies this is to be a global account on the Windows System.

Availability

Secure4Access is currently available for most popular versions of Unix including the following:

Manufacturer	Operating System
Compaq (Digital)	Tru64 (aka Digital UNIX 4+)
Hewlett-Packard	HP/UX 10.0+, 11+
IBM	AIX 4+, 5+
Linux 7	Linux
Sequent	DYNIX/ptx 4+
Silicon Graphics	IRIX 6.5+
Sun	Solaris 2.5+ (Sparc and Intel)

Secure4Access ageNT: Windows NT™ 4.0+.

To obtain a copy of Secure4Access to evaluate on your system visit us on our web page:

http://www.s4software.com

or send email to our sales department:

sales@s4software.com

Be sure to include your operating system type and full name and address for delivery.

Or call us:

S4Software, Inc.(858) 560 - 8112