Authentication Services
Part of the HP ProtectTools portfolio

User credentials are a vital part of your defence. Any compromise and your organisation becomes exposed to the intruder.

Unauthorised access to your company’s computer systems presents a major threat to security. Individuals with limited skills and experience can download tools which can be used to spearhead all kinds of attacks on your systems.

HP ProtectTools Authentication Services provides features that guard against attacks and unauthorised access.
HP ProtectTools Authentication Services algorithms are approved by UK Government.

Key features
- Password Hashing with UK Government approved algorithm
- Customisation values ensure each organisation’s system is unique
- Salting of user credentials produces unique password hash
- Password Management
- Login Auditing
- Auto-logoff Screensaver
- Password Generation System
- Minimal impact on the user

Password Hashing
When a user logs into their account, they enter a username and password. A mathematical algorithm is applied to the password they enter in a process called ‘password hashing’, resulting in a number or ‘hash’. It is this hash, and not the actual password, that is compared to that stored by the Operating System.

This hashing process is one-way and as such the original password cannot be derived from the hash. However, if the algorithm used to create the hash is known, it can be used as the starting point for an attack against user accounts. HP ProtectTools Authentication Services removes this threat, using an algorithm which is seeded with a CESG or customer provided unique value, making every installation different.

The passwords are “salted” with the username and a once only value. The result of this is that two users setting the same password generate different password hashes.

Password Management
To prevent users setting weak passwords, HP ProtectTools Authentication Services contains an optional Password Generation component. When prompted to change password the user is asked to choose a password from a number of generated passwords. All HP ProtectTools Authentication Services generated passwords are produced with approved algorithms in three configurable formats:
- Sentences (Pass Phrases)
- Random Words
- Clearview (CVC-CVC-CVC)

These are easy to remember pronounceable passwords.

Auto-logoff Screensaver
Auto-logoff provides an Auto logout Meta Screensaver that can be configured to automatically log off the user after a period of inactivity. This Meta Screensaver still allows other normal screensavers to run and lock the workstation.
Login Auditing

Last Login Information is the first line of detection of unauthorised access attempts. When a user logs in the system presents the user with the date, time and workstation of the last successful and unsuccessful attempt, along with the number of failed logins since last login. If the user notices that this information does not match what they expect, they can alert the system administrator to a potential security breach.

Unlocking a workstation will also provide the user with the number of failed unlocks which they can act upon.

The Last Login Information is stored in a centralised database which can be used to enforce further security within your environment.

It is not uncommon for users to share usernames and passwords with colleagues to expedite a task. This may get the job done quicker, but it becomes difficult to ascertain who has done what.

Using the centralised Last Login Information, HP ProtectTools Authentication Services can deny multiple concurrent Logins within the domain. This prevents users logging on from multiple PCs and helps maintain individual accountability.

Password Generation System

To complement HP ProtectTools Authentication Services there is HP ProtectTools Password Generation System. This is installed on workstations throughout your organisation to make sure local administrator passwords are changed automatically at regular intervals. The password is created using a hashing algorithm fed with the username, workstation name, date and a shared secret. Each workstation’s privileged account is protected by a regularly changing unique password, yet administrators can readily re-generate the correct password when they need to login.

System Pre-requisites.

- Microsoft Windows® 2000
- Microsoft Windows® XP (32 and 64-bit)
- Microsoft Windows® Server 2003 (32 and 64-bit)
- Microsoft Windows® Vista (32 and 64-bit)
- Microsoft Windows® Server 2008 (32 and 64-bit)

Installation, Configuration & Upgrading

For security reasons, HP ProtectTools Authentication Services is supplied in a non-configured form. This enables customers to configure and create their own distribution kit, customised for their particular site requirements.

With the advent of the latest UK Government algorithm, HP ProtectTools Authentication Services v4 supports parallel upgrade from v3. This new upgrade capability enables a smooth transition from old to new with minimal user impact and password resetting.
HP ProtectTools is a suite of products that provides Authentication, Data and Email Security that can be configured centrally but enforced across the enterprise.

**Enterprise Device Access Manager**
Centralised control of devices within your organisation be it a storage device, e.g. USB pen drive, CD/DVD; or a device that extends the boundaries of your network, for example, bluetooth, wi-fi, InfraRed, provides read/write control of removable disk drives and CD/DVD drives. Device access control policy is set, stored and propagated using standard Windows® features.

**Email Release Manager**
Enforces an enterprise-wide email security policy. Centrally defined, but applied locally when the user presses ‘send’, the email security policy controls who can send what to whom based on Security Labels, Rules and Destinations. When emails are sent, HP ProtectTools Email Release Manager can force auditing, digital signing and encryption. Mail Calming functionality can prevent unwanted email storms.

**Role Based Access**
Integrates with standard Windows® facilities to allow users to access multiple domains from a single workstation whilst maintaining cryptographic separation between data. This allows organisations to maintain the required level of security whilst removing the need for multiple desktops per user. Roles instead of Windows® accounts can be used to determine application and data access making user provisioning simpler.

HP ProtectTools Authentication Services includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. [http://www.openssl.org](http://www.openssl.org)

---

**HP ProtectTools Authentication Services is just one of a range of security solutions. For further information; Tel: +44(0) 1925 841881 or Email: protecttools@hp.com**

To learn more visit: [www.hp.com/services/protecttools](http://www.hp.com/services/protecttools)

---

© Copyright 2010 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Microsoft and Windows are U.S. registered trademarks of Microsoft Corporation

4AA1-1463EEE, Created June 2010