HP ProtectTools Multi-Factor Authentication

User credentials form a vital part of your security controls. Compromised user credentials give unwanted intruders access to your systems and to your valuable data. In today's world, authentication using only a password is not always enough.

HP ProtectTools Multi-Factor Authentication provides security enhancements to the Microsoft® operating system by forcing users to successfully provide multiple independent factors of authentication before they are allowed access to a Windows® desktop.

The different authentication factors can be a combination of something you know (username/password), something you have (token) and something you are (biometric).

HP ProtectTools Multi-Factor Authentication ‘chains’ the different authentication factors and navigates the user through each factor. If the user satisfies each of the different authentication factors such as Username/Password and Smart card/PIN, they will be granted access to their desktop session. If the user fails to satisfy one or more of the authentication factors, access is not granted.
Independent Multi-Factor Authentication

Multi-Factor authentication is defined as a combination of something you know, something you have and something you are. How this is interpreted and implemented varies which results in varying levels of security for your authentication system. Whilst smart card (something you have) and PIN (something you know) meets the definition of multi-factor authentication from a users point of view, does it truly form constituent Multi-Factor Authentication within the authentication system? When using smart card/PIN on its own, the authentication system still only performs one authentication check using the digital certificate stored on the smart card.

With HP ProtectTools Multi-Factor Authentication several independent authentication factors are checked by the operating system. When using the combination of username/password (both being something you know) and smart card/PIN (something you have and something you know), the Username/Password is one independent authentication check and smart card/PIN is a second independent check.

Smart card/PIN, on its own, is analogous with needing one key to open a door. HP ProtectTools Multi-Factor Authentication requires two different keys to open the door.

Authentication Experience

When using Multi-Factor Authentication, at least two authentication factors are required to gain access to the Windows desktop. Each authentication factor causes a credential ‘tile’ to be sequentially displayed to the user. Whilst the user sees an increase in the number of credential tiles that they need to navigate through, the look and feel of each individual tile is identical to that which would be displayed by the operating system if HP ProtectTools Multi-Factor Authentication was not installed.

The user will enter credentials for each tile they are presented with. Once all credential tiles have been completed, Multi-Factor Authentication will determine whether the logon has been successful or has failed. A successful logon allows the user to create a new Windows desktop session or connect to an existing one.

A logon attempt fails if the user provides invalid credentials to one or more of the credential tiles they have been presented with. Aligned to best security practice, neither the user experience nor messages displayed to the user will indicate which of the authentication factors have failed.

The above process will also be enforced during the unlocking of a Windows desktop session.

Multi-Factor Authentication leverages existing Windows Credential Providers to minimise user education and to deliver an enhanced authentication experience without affecting Windows authentication policies. For example, removal of the smart card from its reader during an active session will continue to lock the session.
Passwords & PINS
An important feature of Multi-Factor Authentication is that it complements existing Windows authentication without affecting standard features. As passwords and PINs play a key role in authentication, it is imperative that the user and administrator mechanisms for controlling them remain the same.

Multi-Factor Authentication does not modify the process by which a user can change their password or PIN. Users can change their password and smart card PIN using the standard Windows mechanisms such as the logged in secure authentication sequence accessed through Ctrl+Alt+Del.

Handling of password expiry & blocked smart cards
In most systems, passwords are valid for a specific amount of time, after which a user will be prompted to change the password. If the password is not changed it will be considered expired and logon attempts using that password will fail.

Smart cards use a PIN to provide access control to the digital certificate(s) stored on the card. Should an incorrect PIN be entered more than a configurable number of times, then the smart card will be blocked.

Multi-Factor Authentication has been designed to handle both expired passwords and blocked smart cards without compromising the integrity of your system. In cases of expired passwords and blocked smart cards Multi-Factor Authentication ensures that an attacker will be unable to leverage expired passwords or blocked smart cards to obtain information concerning the users' credentials.

Cached Authentication for offline access
Microsoft Windows caches users’ logon information locally to permit logon should a domain controller be unavailable during later logon attempts. Multi-Factor Authentication supports the use of cached logons for the standard username/password and smart card/PIN combination.

Single factor override based on Policy
When using Multi-Factor Authentication, multiple authentication factors will be used by default. However, there are circumstances where the use of multiple authentication factors will not be possible, for example when a user needs to authenticate but has lost or forgotten their smart card.

In these circumstances, a policy can be configured centrally by an administrator to permit authentication using a single factor only. This policy can be configured to affect specific users, specific systems or both. The centrally defined policy is stored in Active Directory and utilises the built in features of AD to propagate settings throughout the domain.

Single factor override provides business benefits by enabling users who have lost or forgotten their smart card to be able to logon and work using a single authentication factor on a temporary basis. This feature can also be utilised during product rollout where smart card provisioning may be phased and were the number of factors required is determined by the location of the user access device.

Remote Desktop Support
Organisations in every sector are increasingly embracing the advantages of remote computing to reduce costs, simplify provisioning and improve levels of security for their data.

Remote computing requires the use of a remote desktop client to access a remote desktop session being hosted by a virtualisation or server based computing technology. HP ProtectTools Multi-Factor Authentication can be used to enhance the authentication of a remote desktop in much the same way it can be used to access a local desktop session. The user will need to successfully provide multiple authentication factors before they are allowed access to the remote desktop.

The key features of Multi-Factor Authentication are:
- Provides Windows desktop Multi-Factor Authentication
- Chains together two or more independent authentication factors
- Gives no indication of failing factor
- Administrative single factor override based on policy
- Supports cached Authentication for offline access

System Pre-requisites
- 32 bit - Vista, Win7, W2K8, WES7
- 64 bit - Vista, Win7, W2K8, W2K8R2
Authentication factors
The architectural approach within Multi-Factor Authentication enables the product to leverage credential providers of other suppliers. Username/Password, Smart Card/PIN and Biometrics can all be catered for in HP ProtectTools Multi-Factor Authentication.

HP ProtectTools Multi-Factor Authentication is hardware and software agnostic in terms of the authentication factors it will support. The product is software only giving customers the flexibility to choose the tokens and supporting hardware they wish to implement for their different factors.

Further safeguard your systems with HP ProtectTools Authentication Services
To further protect your data, Multi-Factor Authentication can be complemented by another authentication product from the HP ProtectTools suite. HP ProtectTools Authentication Services addresses the security threat of unauthorised access to Microsoft Windows computer systems by providing the feature of replacing the standard Windows password hashing algorithm.

In addition to the replacement algorithm, Authentication Services contains a Password Generation feature to ensure the use of strong, machine generated passwords. It also provides ‘last logon’ information which provides early warning of potential intruders attacking your systems.

For UK Government and Public Sector customers who need to meet the security requirements of CESG, HP ProtectTools Authentication Services replaces the standard Windows password hashing algorithm with a UK Government CESG-approved password hashing algorithm. Using a combination of HP ProtectTools Multi-Factor Authentication and HP ProtectTools Authentication Services will enable customers to meet many of the policy requirements of CESG Information Assurance Standard No.7, Authentication of Internal Users of ICT Systems Handling Government Information (IA57).

HP ProtectTools is a suite of products that provides Authentication, Data and Email Security that can be configured centrally but enforced across the enterprise.

Authentication Services
Enhances the standard Microsoft authentication process with a UK Government approved Password Hashing algorithm. Different inputs are provided to the hashing component to provide site specific password hashes. Password Generation (including Pass Phrases) forces users to select strong, machine generated passwords while Last Login Information warns that your system has come under attack.

Enterprise Device Access Manager
Centralised control of devices within your organisation be they a storage device, e.g. USB Pen Drive, CD/DVD, or a device that extends the boundaries of your network, e.g. 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, 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

HP ProtectTools Multi-Factor Authentication 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

*CAPS evaluation of HP ProtectTools Multi-Factor Authentication did not cover Biometrics.