Advanced User Identification and Access Control
For the Enterprise Market
Utilizing Common Login Methods

The Autoload Password Manager
With Policy Master Configuration Utility

Policy Master v2.2.0
The World’s First Password and Login Management System

Mandylion Research Labs
www.mandylionlabs.com
# Index

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Getting To Know The Autoload Platform</td>
<td>3</td>
</tr>
<tr>
<td>Features and Benefits</td>
<td></td>
</tr>
<tr>
<td>Tokens, Cradles &amp; Configuration Software</td>
<td></td>
</tr>
<tr>
<td>Cautionary Notes on Password Usage</td>
<td></td>
</tr>
<tr>
<td>Using the Autoload Token</td>
<td></td>
</tr>
<tr>
<td><strong>Initial Setup</strong></td>
<td>7</td>
</tr>
<tr>
<td>System Requirements</td>
<td></td>
</tr>
<tr>
<td>Loading Policy Master Utility Software</td>
<td></td>
</tr>
<tr>
<td>Installing Configuration Cradles</td>
<td></td>
</tr>
<tr>
<td>Initializing Tokens</td>
<td></td>
</tr>
<tr>
<td>Control &amp; Distribution of Configuration Software</td>
<td></td>
</tr>
<tr>
<td><strong>The Policy Master Software</strong></td>
<td>11</td>
</tr>
<tr>
<td>Working with Templates</td>
<td></td>
</tr>
<tr>
<td>EZ-Autoload Utility for End Users</td>
<td></td>
</tr>
<tr>
<td><strong>Setting User Information</strong></td>
<td>13</td>
</tr>
<tr>
<td>Naming Templates</td>
<td></td>
</tr>
<tr>
<td>Entering Individual or Class of User Information</td>
<td></td>
</tr>
<tr>
<td><strong>Setting Enterprise Defaults &amp; Locks</strong></td>
<td>13</td>
</tr>
<tr>
<td>Alarms and Lockout Policy</td>
<td></td>
</tr>
<tr>
<td>Default Password Generation</td>
<td></td>
</tr>
<tr>
<td><strong>Creating Login Records</strong></td>
<td>14</td>
</tr>
<tr>
<td>Identifying the System</td>
<td></td>
</tr>
<tr>
<td>Defining Password Policy</td>
<td></td>
</tr>
<tr>
<td>Defining Initial Settings</td>
<td></td>
</tr>
<tr>
<td><strong>Downloading to the Autoload Token</strong></td>
<td>17</td>
</tr>
<tr>
<td>Downloading as an Administrator</td>
<td></td>
</tr>
<tr>
<td>Downloading as an End User</td>
<td></td>
</tr>
<tr>
<td><strong>Advanced Applications</strong></td>
<td>19</td>
</tr>
<tr>
<td>Associating Tokens with Templates</td>
<td></td>
</tr>
<tr>
<td>Group Passwords</td>
<td></td>
</tr>
<tr>
<td>EZ-Autoload Utility for End Users</td>
<td></td>
</tr>
<tr>
<td><strong>Token Behavior Matrix</strong></td>
<td>23</td>
</tr>
<tr>
<td><strong>FAQ’s</strong></td>
<td>24</td>
</tr>
<tr>
<td><strong>General Information &amp; Technical Data</strong></td>
<td>34</td>
</tr>
<tr>
<td><strong>Warranty Information</strong></td>
<td>35</td>
</tr>
</tbody>
</table>
Passwords are the most common form of personal identification in use today. They have become an important part of the routine in our daily lives. We have come to accept this annoying and imperfect little form of identification. We intuitively assume passwords provide us with adequate security. The experts know differently. *Hackers just snicker.*

The Autoload Platform is the next generation of Mandylion’s password management token technology. The Platform consists of Autoload Tokens, Policy Master Configuration Cradles and the Policy Master Configuration Software Suite.

The Token has been designed from the ground up for the way we access and use password controlled applications. It does away with the inherent weaknesses associated with passwords; the reliance on the individual to create, remember and regularly change them.

Truly an enterprise management tool, the autoload version allows organizations to configure and control the token on behalf of the organization’s users. The organization can set and control the enterprise logins and yet still allow the user to maintain their own personal logins on the token. Mixing official and personal logins provides a benefit to the organization; It promotes a culture of security over password use.

---

* Designed in conformity with U.S. Military, National Institute of Standards and Technology and National Security Agency standards for the secure creation, management and use of passwords. All units comply with DoD information security guidelines D8500.1 and D8500.2; US Army Regulation 251A; FIPS Pub. Nos. 112, 190 and 196 and NIST Special Publication 800-63 titled “Electronic Authentication Guideline. (9/04); NSA and Committee on National Security Systems (CNSSS) National Security Telecommunications and Information Security Systems Policy No. 11 (NSTISSP #11).
**Features & Benefits**

Securely Stores up to 50 passwords. Along with account numbers and website / application names.

Generates Strong Passwords. Patent pending kinetic circuitry actually senses your use of the unit. This aids the unit’s processor in the generation of strong passwords which thwart all known password cracking techniques including dictionary and brute force approaches. Passwords can be any length up to 14 characters or namespaces.

Preconfigurable. Can be configured by the organization on behalf of the user. Handles incremental updates as well as group passwords. The enterprise can control what the user can modify on the token.

It’s Automatic. Prompts you to change your passwords at preset intervals, then can automatically create a new one for you.

Tamper Resistant. Only the authorized user it is assigned to can turn it on. Circuitry is designed to thwart electronic bypass. Unit has user selectable lockout settings including a self destruct function.

No Software needed. Nothing to Install. Simple read out can be instantly used with any Web site or system.

Carefree Operation. Uses standard batteries. Batteries last about a year with daily use. All passwords and settings are stored in permanent and protected memory which is unaffected by battery life or loss of power.

Configuration Utility and Cradle. The autoload version of the token can be configured either manually on the token itself or via the Policy Master Configuration Utility and downloaded to the token.

Operation is Simple and Intuitive. You can use it to add convenience while improving your security anywhere you use passwords, PINs or pass codes.

---

**Getting to Know the Autoload Platform**

(continued)

**Ease of Use**

To use the token with your logins, you simply follow three easy steps:

- Access the password input area or screen of the Web site or system you wish to gain access to.
- Activate your token and display the stored password or memory aid to arrive at the password that you created for that site.
- Enter the password* in the input area of the Web site or system as you normally would ...and you are in!

Using the token instantly provides you with a quantum leap in security protection.

---

* For an even greater defense-in-depth security over your passwords, use the device as a memory aid to recall your actual passwords. A simple offset technique can apply something only you uniquely know to the characters displayed, to arrive at the actual password. Under this method, the passwords are never stored within the token. The device functions as a memory aid to arrive at the correct password. See FAQ’s for detail on the technique.
Cautionary Notes on Password Usage.

According to the annual FBI “TOP 20 LIST”\(^1\), humanly generated, easily crackable passwords are the greatest vulnerability associated with today’s password usage.

In environments where users are either uncomfortable or further, prohibited from writing down or electronically storing their passcodes, the token may be used as a memory aid for the management and recall of strong passwords.

To use the token in this mode, the principle of offsets is used. Rather than the token displaying and storing the actual password for a Login Record, a simple offset technique can apply something only you uniquely know to the characters displayed, to arrive at the actual password. This way the password is never stored. If the token contents were somehow revealed, they would still be unusable.

The lockout features and tampered alarms of the token, although strong, are merely deterrents to wrongful access and compromise of the device. They are part of the device's "defense in depth" strategy. When combined with the other features, controls and recommended use and possession of the device, they create a formidable barrier to wrongful access of the device.

It is always theoretically possible to defeat a singular security control, such as lockout, given enough time and persistence. Accordingly, relying on a single security feature in isolation of these other controls is not recommended. In high risk environments, Mandylion strongly recommends that users keep their tokens in their possession, remain vigilant as to possible signs of tampering and utilize the token as a memory aide (see FAQ’s)

---

About the Display...

The Display has Three Information Areas

...and the Manual User Interface

Only 5 Keys Control the Entire Unit:

Four Directional Arrows surrounding a center Enter/Select Key.

Using the Autoload Token

Presented below is a simple overview of the Autoload token. For full details on the use and manual configuration of the token, please see the separate manual titled the Autoload User Guide.

Note: The above symbols are used throughout this guide to represent the keys. The ▲ symbol indicates pressing the up and down arrow keys simultaneously. (Only used to switch between View, Edit and Options Modes.)
**System Requirements:**

To install and operate the Mandylion Policy Master Utility Software for the Autoload token, the system must meet the following requirements:

- Win7, VISTA, Windows XP, 2000, NT, 98, 95 Operating System;
- Wintel Pentium hardware platform;
- 10 MB available hard disk space;
- VGA monitor with 1024x 768 minimum resolution;
- CD-ROM drive;
- Mouse;
- USB port;
- Mandylion Policy Master Token Cradle; and
- Mandylion Autoload Token.

**Installing the Policy Master Program**

Double click on the Setup.exe icon and follow the instruction steps. (important: run setup.exe before plugging in cradle)
Installing the Policy Master Program (con’t)

A welcome message will appear:

- Click “Next”

Choose Destination Location (default is program files):

- Click “Next”

Choose Program Grp (default is Policy Master):

- Click “Next”

When installation is complete:

- Click “Finish”
The Policy Master Setup.exe creates the following files and folders and deposits them into a newly created directory C:\ Program Files\ Policy Master.

Note: If you are upgrading from a previous version of Policy Master (which is required for the desktop personal cradle) your “accounts” folder and its contents will remain but all other files will be replaced.

To completely deinstall the Policy Master application and remove it from your computer, click the “UNWISE” application in the Policy Master Folder. This deinstall process will preserve any accounts that had been set up in the accounts folder but remove all other files.

Questions or help with the installation process can be obtained via the mandylionlabs.com web site or by calling Mandylion directly from the contact numbers on the web site.

Installing the Configuration Cradle

Once the Policy Master Program has been installed, the desktop personal cradle can be plugged into any available USB port to commence its installation.

The cradle is a serial device that communicates through the USB port. It requires two drivers to be installed via the Windows Operating System “Hardware Wizard”.

Plug the cradle into any available USB port and the following hardware windows will appear in sequence:

The Windows New Hardware Wizard will then automatically install the necessary drivers.

When complete, the New Hardware Wizard will provide a notice that the device is ready for use.

The Installation of the Configuration Cradle is now Complete.
Initializing Tokens

Tokens are licensed for use in conjunction with the Policy Master Software license. Each token must be initialized by the Policy Master software prior to its first use.

Initialization is a one time, one step process. It is performed by placing a new token in the configuration cradle and running the initialization utility which comes with the Policy Master configuration software.

This utility invokes the DESTROY command and completely resets the token to its default state.

NOTE: All data that may have been contained in the token is irretrievably erased and destroyed with this initialization process. Additionally, this process embeds the serial number of the Policy.

Control and Distribution of Configuration Software

The Policy Master Software license allows the token to be configured by that software.

NOTE IF YOU ARE UPGRADING FROM A PREVIOUSLY INSTALLED VERSION OF POLICY MASTER – USE YOUR OLD LICENSE NUMBER OR THE SOFTWARE WILL NOT RECOGNIZE YOUR TOKENS.

NOTE FOR ENTERPRISE USERS

The Policy Master Configuration software suite provides the enterprise with a great degree of control and authority over each token that is licensed to it. Except for the Policy Master Public Utility which can be freely distributed due to its limited configuration capabilities, the entire Policy Master Configuration software suite should be controlled by the enterprise and only provided to enterprise personnel assigned to the configuration and support of end users.

If control among token administrators is sought by the enterprise, the Policy Master software has a unique ability to associate and control specific tokens by administrator or group administrators. See the Advanced Applications section of the manual on association and group association of tokens.
The Policy Master Configuration Software
Working with Templates

The Policy Master Configuration Software is a template based application. It provides a great deal of “cut and paste” flexibility in creating login records for a single token or multiple tokens for whole classes of users. (See Advanced Applications) The basic Policy Master Template screen is shown below. This is the default file which appears on the screen when the application is launched. The template is divided into three logical areas; user information input area; selection of default parameters to the device including locks, alarms and default password generation; Login Record Area.

The Login Record Area scrolls to display entry for all 50 login records. Each Login record is divided into three sections; System Definitions; Policy Description; Initial Settings. Lock icons allow the administrator to enable/disable the ability of the user to change a particular field on the token. Record Selector indicates which records are to be updated/downloaded to token on an incremental or full update/download.
EZ-AutoLoad Utility for End Users

The Mandylion autoload token contains capacity for up to 50 simultaneous login records. In most instances, this capacity is more than adequate to accommodate all of the average user’s corporate logins as well as the user’s personal logins. To promote a culture of security within their organization as well as reinforce familiarity with the operational use of the token, the enterprise and corporate administrators should encourage their users to use this excess capacity for their personal logins.

To that end, the Policy Master Configuration Software includes a utility which can be provided to token users for the configuration of their own personal password records. This utility is known as Policy Master Public. It is a small executable which contains only a subset of the features and configuration capabilities of the main Policy Master template. This utility is designed to be loaded either on an end user computer, or alternatively, in a kiosk type environment.

*Please Note:* Enabling user access to configure or change login records is strictly an enterprise policy decision. As discussed in the previous section, if an organization does not wish their users to utilize the token except for the enterprise’s login records, the token can be set administratively to lock off the user from any “on token” or “on cradle” configuration privileges.

For details on the features and use of the Policy Master Public utility, see section “Advanced Applications.”
Setting User Information
Naming Templates

The Policy Master Configuration template can be saved for an individual user or generated and saved for a group of users which share similar access privileges. To name a template and save it in the “accounts folder”, select from the Account Menu “save” or “save as”. Flexibility is provided for administrators to be able to create and save templates in accordance with their organizations needs. All Policy Master Configuration templates carry an “.ebp” windows file extension.

Entering Individual or Class of User Information

The User Information Input area contains 6 fields of static information which helps identify a particular template and associate it with a particular individual or group of individuals. Entry of data into these fields is strictly optional on the part of the administrator. No user data contained in this area is downloaded to the token.

The form allows the administrator to enter Roles, the users name and Title, supervisor information as well as security officer points of contact, if any, assigned to that individual or group of individuals. An overrideable system field records and keeps the initial creation date of the form.

Setting Enterprise Defaults and Locks
Alarms and Lockout Policy

The autoload token possesses several tamper alarms, lockouts and limits on failed login attempts. These alarms and lockout policy can be set and controlled by the administrator and/or the user. The logical and physical controls over access to the token form a defense in depth approach to controlling the authorized use of the token.

Locks can be set for the number of failed attempts to gain access (1, 3, 5 or 10 tries) as well as the sanction if those limits are exceeded (various time lockouts through complete overwrite, destruction of entered data and lock of the token). Administrators can enable/disable the ability of the user to change the lockout parameters on the token.

Default Password Generation

For convenience, each autoload token has a default password schema and renewal parameters which is utilized when a specific password policy is not defined for a particular login record. Administrators set the default password generation parameters on the template and can enable/disable the ability of the user to change these parameters on the token.
Identifying the System

To identify a particular login record, the template provides three downloadable input fields. Each is 14 characters in length. The first field describes the Login Record’s name (i.e. email, or VPN etc); the second field is available to enter an account number, screen name or user ID associated with the login record and finally, there is a field to enter technical or help desk telephone numbers associated with the login.

Administrators set the system definitions for each login record and can enable/disable the ability of the user to change these identifiers on the token.

Defining Password Policy

For purposes of the template, password policy is defined as the schema or composition of the password required by the login and its renewal.

User passwords can be specified by length, composition and renewal interval. Composition or schema of each password can be specified down to the keyspace (position) within the passcode to be generated. Composition can be randomly drawn from the entire printable ASCII character set (base 94) or throttled to any or a combination of the following subsets of the printable ASCII character set:

- Upper Case Letters (base 26)
- Lower Case Letters (base 26)
- Upper and Lower Case Letters (base 52)
- Numbers (base 10)
- Special Characters (base 31)
- Any but Special Characters (base 63)
- National Character Set (#;$,@)
- Upper Case Alpha and Numbers (base 36)

The following options can be enabled or disabled by the Administrator in the creation of a password’s composition, by login record:

- Minimum length; Maximum length;
- Password to be totally random; i.e. cannot contain the username or word;
- Can specify minimum representation of each ASCII character set;
- Password must contain a configurable number of numeric characters;
- Password must contain a special character (from a customizable list);
- Password must contain at least one lowercase character;
- Password must contain at least one uppercase character;
- Password cannot be set to a previously used password;
- Password cannot contain any variation of the users name;
- Password cannot can not be a dictionary word.

Password schema is created by making a selection from the pull down menu in the “Schema” column of the Policy section. Selections are Default, Structured, Randomized and Manual.
Selecting the Structured Option in the pull down menu displays a preference box which allows the administrator to set the token to generate a purely random password of a specific length for that specific login record.

With this option, the device’s random number generator can be further throttled to only generate specific subsets of the ASCII character set in each position within a particular password. This feature allows for the creation of passwords that fit the schema requirements of applications/hosts which might require, for instance, only an alphanumeric in the first position of the password.

Selecting the Randomize Option in the pull down menu displays a Preference Box that sets the token to generate a purely random password of a random length within a specified minimum and maximum length range for the login record selected. This option also allows the administrator to set the minimum and maximum count of characters within the password from specific subsets of the ASCII character set.

Unlike the Structured Option, this option calls on the powerful random number generators to select the position within the password of where these specific character sets will fall.
Selecting Manual in the pull down menu displays a Preference Box which allows for entry of a manual or previously generated password. A manual password may also be entered into any record as its password of record or as an initial bootstrap, one time password.

Intervals included in the standard configuration are:

- Upon First Use
- 30 Days
- 45 Days
- 60 Days
- 90 Days
- 180 Days
- One Year
- Two Years
- Never

Mandylion autoload token allows for a “grace period” for password change to accommodate synchronization with other logins and applications as well as to temporarily delay password updates to a more convenient time to the user.

**Defining Initial Settings**

The Policy Master Configuration software has the ability to not only set the parameters for the ongoing password for each login record but can also control and accommodate the definition of the “bootstrap” or “Expire on First Login” policy for that record.

The administrator has the option of setting the Expire On First Login password to expire upon first use and automatically generate a new password for the user that complies with ongoing policy. Alternatively, the Expire On First Login password can be delayed to first policy change date or held static, as in the case of group or manual password login records.

Individual passwords can be set to be generated by the device or securely loaded via the cradle from the individual template by login record. This latter feature allows for the input of host generated passwords or group passwords and their coordination among users.
Once a template has been defined for a particular user or class of users, it can be downloaded to an Autoload token. Downloading is accomplished via a Policy Master Configuration Cradle.

The download process is quick and the average token can be configured in less than 10 seconds.

Flexibility is provided for administrators to be able to create and save templates in accordance with their organizations needs and download to the tokens as needed.

Tokens can be configured by administrators prior to their initialization by the end user.

When provisioned with a token, all the user has to do is create their own fingerpattern for access and they are done! This constitutes the initialization process by the user.

Unused login records can be set by the administrator to allow for the user’s personal use. Alternatively, a user can configure their own token from their own PC or a shared “kiosk” type station without the assistance of an administrator. (See EZ-AutoLoad Utility for End Users – See Advanced Applications)

Due to a unique lockout control, Login records set by the enterprise cannot be reconfigured or erased by the user. Login records set by the user can be overwritten by the enterprise, however, they cannot accessed by the enterprise.
On the back of the autoload token there are 4 ports which connect the token with the “pogo pins” on the face of the Policy Master Configuration Cradle.

From a security design perspective, no bilateral communication occurs between the token, the Policy Master cradle and the Policy Master Software in the download process.

All downloads constitute “unidirectional writes” of data streams which are either accepted or rejected by the token based upon the criteria established in the token. As a safeguard, the Policy Master configuration software and templates cannot interrogate a token for its contents or state. If an administrator is unsure as to a token’s origin, the administrator’s only option is to DESTROY, reset and reinitialize the token. (See Initializing Tokens)

**Proper Placement of Token on Cradle**

The token should just “snap” into the cradle and make direct contact with the “pogo pins” on the cradle. A specially designed channel at the bottom of the cradle allows the token to be placed on the cradle while on a keyring.

If properly positioned on a plugged in cradle, the token LCD will remain blank or display what the token normally displays off the cradle ( “Enter Code” or New Code or View, etc.) Only when downloading will the token read “Ready” indicating that the token has been properly mounted and is ready for downloading and is receiving a download.

If you do not see “Ready” on the token’s LCD while in the actual act of downloading to the token, attempt the mounting process again to ensure the ports on the token are aligned over the “pogo pins” on the cradle.

If the token is still not in “Ready” mode, make sure that the cradle is plugged into the USB port of your computer and that the token is operative. Taken off the cradle, a properly operating token will read either “New Code?” or “Enter Code” on the LCD when the enter (center) button is depressed.
The Policy Master Configuration software suite provides the enterprise with a great degree of control and authority over each token that is licensed to it. Except for the Policy Master Public Utility which can be freely distributed due to its limited configuration capabilities, the entire Policy Master Configuration software suite should be controlled by the enterprise and only provided to enterprise personnel assigned to the configuration and support of end users.

In certain environments, token administrators may wish to associate a specific Policy Master template that they have created with a particular token or class of tokens.

This association is a “hard” physical association. It binds the Policy Master Template created with the token(s) it has been downloaded to. It differs from naming and saving a “default” Policy Master Template file in the name of an individual, class of user, etc. (see Policy Master Configuration Software – Working with Templates) in that once a token and particular template have been associated, only that unique template file will be able make changes and add login records to the associated token(s).

A token can be associated with only one Policy Master Template at a time. Association, however, does not preclude group records from being added or changed to unassigned login records. Further, association does not preclude the end user from adding and changing their own personal logins to previously unassigned records, if that permission had been granted to them by the administrator.

**Note:** Association of tokens is an advanced application and is not recommended for routine token use.

*The advantage of this association is strictly administrative in nature only.* It does not necessarily enhance the security of the underlying token’s use and can actually increase the complexity of token administration. This association merely precludes an overwrite of any of the corporate logins that have been changed by another properly licensed Policy Master Template. A token can be associated with only one Template at a time. Once an association is made, it cannot be reversed. If a token’s alarms/sanctions are activated and the DESTROY function invoked, the token’s contents and settings will be erased, however, it will still remain associated with that particular template. If an association is no longer desired or needed, the only way to reset the token is to re-initialize it using the Initialize Utility. This action will not only terminate the association that had been established, it will also DESTROY the contents of the token. The token will be reset to its factory defaults.

To associate a particular Policy Master Template with a token, select from the “Associate” menu on any Policy Master Template the “Individual Form with Specific Token” option. This association can be initiated at any time in the creation of the Template.

Once an association is made, the status in the header area will change to Associated (pending) and the header information of the Template will change color indicating that you are now working with an associated form. Further, the Associate menu will no longer be operative and indicate, via a check mark, that the Template association has been selected. As a safeguard to keep the associated form in sync with the corresponding token, the “download only” menu choice is disabled from the Account pull down menu and download and save is now the only download option.

Inputting login record parameters into an associated template is identical to the default Policy Master Template. (See Policy Master Configuration Software-Working with Templates).

Once an associated Template has been downloaded and bound to a token, its status in the header area will
Advanced Applications
(continued)

change from “Associated Pending” to “Associated”. The act of just creating and saving an associated Template without performing a download does not bind the Template with a token. According, the final status indication of “Associated” only appears upon a download to a token.

Group Passwords

The Policy Master Configuration software suite provides for the efficient and secure administration of group passwords. Group passwords typically occur in multi-server 24/7 uptime environments where a trusted core of administrators are required share root login access. Physical Cipher locks to doors and safe combinations are also considered group passwords. In addition to the access code itself, group passwords may or may not share identical user ID/screen names.

The Policy Master Configuration software suite manages all variations of group passwords and offers a secure method to create disseminate and renew group passwords.

Similar to associating a token with a Template, assigning a token to a group is a “hard” physical association. It binds the Policy Master Template created for that group with the token it has been downloaded to. Unlike creating a Default Template for a class of users that share similar enterprise standard login records, a “Group Associated” template is used by a group administrator to control and administrate a set of previously unassigned login records on a token already under the control of a token administrator.

A token can be “Group Associated” with only one group at a time. By design, group association does not interfere with a token receiving downloads from an administrator using the Default or Associated Template.

A group administrator has secondary authority over the token. As such, downloading a Default Template or Associated Template login record into a “Group Associated” area will overwrite the “Group Associated” login. A “Group Associated” token does not preclude the end user from adding and changing their own personal logins to previously unassigned records if that permission had been granted to them by the administrator.

Note: “Group Association” of tokens is an advanced application and is not recommended for routine token use.

Once a Group Association is made, it cannot be reversed. If a token’s alarms/sanctions are activated and the DESTROY function invoked, the token will still remain associated with the particular group template. If an association is no longer desired or needed, the only way to reset the token is to re-initialize it using the Initialize Utility. This action will not only terminate the association that had been established, it will also DESTROY the contents of the token. The token will be reset to its factory defaults.

To bind a token to a particular “Group” select from the “Associate” menu on any Policy Master Template the “Group with Specific Token(s)” option. This association can be initiated at any time in the creation of the Group Template.

When a Group Association is made, the status in the header area will change to Group Associated (pending) and the header information of the Template will change color indicating that you are now working with an Group Template. Header fields will also change to better accommodate group type
information. Further, the Associate menu will no longer be operative and indicate, via a check mark, that the Group Template association has been selected. As a safeguard to keep the Group Template in sync with the corresponding token(s), the “download only” menu choice is disabled from the Account pull down menu and download and save is now the only download option.

Inputting parameters into an associated template is identical to the default Policy Master Template. (See Policy Master Configuration Software-Working with Templates).

Once a “Group Associated” Template has been downloaded and bound to a token, its status in the header area will change from “Group Associated Pending” to “Group Associated”. The act of just creating and saving a Group Template without performing a download does not bind the Template with a token(s). According, the status indication of “Group Associated” only appears upon a download to a token.

Inputting login record parameters into a “Group” template is identical to the default Policy Master Template with the exception of header information and default password generation. (See Policy Master Configuration Software-Working with Templates).

With a “Group” Template, the header information is tailored to capture information more often associated with a Group than an individual token. Default password generation parameters can be set within a Group Template, however, these parameters will only pertain to the Group Template itself. Default password generation settings on the token can only be Template.

Default password generation parameters can be set within a Group Template, however, these parameters will only pertain to the Group Template itself. Default password generation settings on the token can only be Template.

Advanced Applications (continued)

EZ-AutoLoad Utility for End Users

The autoload token contains capacity for up to 50 simultaneous login records. In most instances, this capacity is more than adequate to accommodate all of the average user’s corporate logins as well as the user’s personal logins.

To promote a culture of security within their organization as well as reinforce familiarity with the operational use of the token, the enterprise and corporate administrators should encourage their users to use this excess capacity in their token for their personal logins. To that end, the Policy Master Configuration Software also includes a utility which can be provided to token users for the configuration of their own personal password records. This utility is known as Policy Master Public. It is a small executable which contains only a subset of the features and configuration capabilities of the main Policy Master template. This utility is designed to be loaded either on an end user computer, or alternatively, in a kiosk type environment.

Please Note: Enabling user access to configure or change login records is strictly an enterprise policy decision. As discussed in the previous section, if an organization does not wish their users to utilize the token except for the enterprise’s login records, the token can be set administratively to lock off the user from any “on token” or “on cradle” configuration privileges.
To use the Policy Master Public utility, a token must not only have been initialized by the enterprise via the initialization utility, it must also have been initialized by the end user.

This utility is secure. Only policy data (length, composition and renewal period of the password) is being transmitted to the token for a particular login record. Data is not cached or able to be saved with this utility. Due to the fact that Policy Master software can only “print” to a token and not interrogate or discern it’s contents, the personal information stored by a user in the token is only known to that user and not to the enterprise or token administrator.

Using the Policy Master Public utility is a snap. All an end user has to do is place their token on a Policy Master configuration cradle, enter their login record data onto the screen and press the “print to token” button. Their token does the rest.

Upon pressing the “print to token” button, the utility will request that the end user enter their finger pattern and place the token in “View” mode. When user acknowledges that the token is in view mode, the data will automatically download to the token.

Note: Two important features to the Policy Master Public utility software safeguard its use. First, unlike the administrator’s templates, the Public utility requires that the user to be present to perform a download. This is because the utility will not “print” to the token unless the token is turned on and in view mode. Secondly, the Public utility cannot alter or overwrite any login record that had been created on the user’s behalf by the token’s administrator.
# Token Behavior Matrix

## Attempting To Download:

<table>
<thead>
<tr>
<th>Default Template</th>
<th>An Associated Template</th>
<th>Group Records</th>
<th>Unclaimed &amp; End User Records</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accepts Download</td>
<td>Accepts Download</td>
<td>Authority Conflict Type C</td>
<td>Authority Conflict Type C</td>
</tr>
<tr>
<td>Authority Conflict Type A</td>
<td>If original associated template - Accepts Download, otherwise Authority Conflict Type B</td>
<td>Authority Conflict Type C</td>
<td>Authority Conflict Type C</td>
</tr>
<tr>
<td>Accepts Download and overwrites Group Login Record(s)</td>
<td>If original associated template - Accepts Download and overwrites Group Login Record(s), otherwise Authority Conflict Type B</td>
<td>Accepts Download</td>
<td>Accepts Download and overwrites Group Login Record(s)</td>
</tr>
<tr>
<td>Accepts Download; Will Overwrite End User entered Record(s)</td>
<td>If original associated template - Accepts Download and overwrites End User entered Record(s), otherwise Authority Conflict Type B</td>
<td>Accepts Download</td>
<td>Accepts Download</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Type</th>
<th>Description of Behavior &amp; Warning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type A</td>
<td>Attempting to &quot;print&quot; to a previously Associated Token using a Default Template</td>
</tr>
<tr>
<td>Type B</td>
<td>Attempting to &quot;print&quot; to a previously Associated Token using a New or Different Token's Associated Template</td>
</tr>
<tr>
<td>Type C</td>
<td>Attempting to &quot;print&quot; to a Login Record previously assigned to a Default or Associated Template using a Group or Public Template</td>
</tr>
</tbody>
</table>
The following is a partial list of Frequently Asked Questions about the autoload token and its use. Further technical information and other FAQs are available at our web site http://niap.nist.gov/cc-scheme/nstissp-faqs.html#Q27 and NSA "Issues in Information Assurance” Guide to NSTISSP No. 11, page 17.

Q. Aren’t Passwords Old Fashioned And Simply Going To Be Replaced Soon?

A. Predictions of the demise of the password method and its replacement with some other form of user authentication are premature. Such predictions are based upon flawed security models which continue to envision the traditional computer/laptop as the common access point to the internet.

Within 5 years, cell phones, pagers and other personal internet access devices (PIAD’s) will provide this access on equal footing with today’s computers. Further, PKI infrastructures are developing that rest on the authenticity of digital certificates empowered by individual user’s passwords. Because the vast majority of these systems seek to be compatible with existing users’ infrastructure, access control will remain a matter of manually “keying in” a shared secret or password.

Q. Under the definitions of Natl. Security Telecommunications and Information Systems Security Policy NSTISSP #11 and the Common Criteria, is the Autoload token an IA or IA enabled product or technology?

A. NO.

According to the NSA “Issues in Information Assurance” Guide to NSTISSP No. 11, under Policy Information and Guidance FAQ #7\(^2\), the NSA definitively excludes the Mandylion technology from being considered an IA or IA enabled product and therefore it is not subject to NIAP.

The Guidance states:

“whether a component is considered an IA/IA-enabled IT component depends heavily on the nature of the architecture in which it is being placed. If the component is not "cognizant" of the security policy and has no security policy enforcement responsibilities (i.e. it is not required to make policy enforcement decisions or implement a security feature), it is not considered to be an IA/IA-enabled IT component and hence will not need to be validated. (“emphasis added)"

Accordingly, under these NSA provided definitions and amplifications of the terms IA product and IA enabled product, the Mandylion technology falls outside of the scope of NSTISSP No. 11.

As in the NSA example provided above, the Mandylion device is not "cognizant" of the security policy and has no security policy enforcement responsibilities (i.e. it is not required to make policy enforcement decisions or implement a security feature) and therefore is not considered to be an IA/IA enabled IT component. Hence does not need to be validated under common criteria certification for its compliant use in certain U.S. Government IT environments.

Q. Is there any specific Federal or DoD Agency Policy Guidance regarding the use of the Autoload Token?

A. YES.

For instance The United States Army Regulation on Information Assurance (AR 25-1A) includes the following requirements under Paragraph 4-12, Password Control:

“The use of password generating software or devices is authorized as a memory aid when it randomly generates and enforces password length, configuration, and expiration requirements; protects from unauthorized disclosure through authentication or access controls; and presents a minimal or acceptable risk level in its' use.”

Q. We are told not to write down our passwords on any media. Can the token help me?

A. Absolutely. According to the annual FBI “TOP 20 LIST”, humanly generated, easily crackable passwords are the greatest vulnerability associated with today’s password usage.

In other words, the risk of physical exposure of an actual passcode is generally considered remote and therefore less of a risk than those inherent with the use of a weak password. The use of the device specifically addresses this threat.

In environments where users are either uncomfortable or, further, might be prohibited\(^\text{1}\) from writing down or electronically storing their passcodes, the token can be very effectively employed as a memory aid for the management and recall of strong passwords to multiple login accounts. The risk of physical exposure to a passcode is generally considered less than the risks inherent with the use of a weak password.

To use the token in this mode, the principle of offsets is employed. With this time proven crypto technique, rather than the token displaying and storing the actual password for a Login Record, a simple offset technique applies something only the user uniquely knows to the characters displayed, to arrive at the actual password.

In this manner, you have two factor authentication; Something You Know, (the offset) and Something You Possess, (the token). With this method, the password of record is never stored or written down. If the token’s contents were somehow revealed, they would still be unusable in obtaining access to the underlying accounts and logins.

Offsets can be either simple or complex. Both are equally effective strategies for a defense-in-depth protection of your passwords. (the token is used to generate and recall strong random strings that thwart brute force cracking attacks waged against the system registries where they are stored in encrypted form; the offsets thwart against its physical compromise of the token by obscuring its contents and the true passcodes.)

A Simple Offset Example –
An example of a simple offset is reading the displayed code backwards. Here, the token’s onboard random number generator creates the strong random string and the offset obscures the string from disclosure.

For instance, lets say a user utilizing the token generates and stores a purely random string of 14 printable characters.

The Display reads:

\[ \text{\textbackslash{}BjrGjh3<u7A&t} \]

---

(http://www.dtic.mil/whs/directives/) states

“Protect authenticators (sic-passwords) commensurate with the classification or sensitivity of the information accessed and share authenticators or accounts only with authorized personnel. Report any compromise or suspected compromise of an authenticator to the appropriate IAO.”

The Directive does not prohibit or impose any other requirements upon the responsible user. Accordingly, for those environments where the classification or sensitivity of the information accessed via the password is unclassified, sensitive “for official use only” i.e. a “prudent manner that prevents disclosure or unauthorized access to them.”
The user secretly applies the following simple offset, only known to him/her, to arrive at the true password for the Login Record:

(1) The password is read right to left;

The actual password for the Login, after applying the offsets would be:

t&A7u<3hjGrjB\  

(User reads display right to left (application of offset)).

**AN EXTREME EXAMPLE** –
The following is an example of a complex offset that combines multiple techniques which can be used separately or in combination with other techniques. This example includes (1) a fractional reading of only a subset of the displayed code; (2) applying multipliers against displayed numeric characters; and (3) substitutions for displayed alpha characters.

For this example, lets say a user utilizing the token generates and stores a purely random string of 14 printable characters.

The Display reads:

\BjrGjh3<u7A&t

The user secretly applies the following complex offsets only known to him/her to arrive at the true password for the Login Record:

**Offset (1):** The password length is only the last 8 Characters read right to left on the display;

**Offset (2):** All displayed alphas are decremented by one character;

**Offset(3):** All displayed numbers are incremented by one.

The actual password for the Login would be discerned in the following 3 step process:

Step 1: - Locate the Last 8 Characters of the displayed password and read them right to left.

t&A7u<3h

Step #2: All displayed alphas are decremented by one character (application of offset #2):

s&Z7t<3g

Step #3: All displayed numbers are incremented by one character (application of offset #3):

s&Z8t<4g

Under this complex example, the displayed password of \BjrGjh3<u7A&t would be converted by the user to the actual password of

s&Z8t<4g

Without knowledge of the offset only known to the user, it is impossible to deduce the actual password from the displayed password.

As stated above, offset techniques can be simple or complex. They are, however, easier to remember and apply to multiple strong passwords than memorizing and frequently changing and re-memorizing the underlying strong password itself.

**Q. I know that storing passwords on my PC is not prudent. Currently, I use a Palm Pilot type PDA to store my passwords. Why should I use a Mandylion Password Manager?**

**A.** Even if you own and use a PDA, there are four important reasons why you would still want to use a Mandylion Password Manager:
First, its purpose. Your PDA is not a special purpose access control device. It is used for many different tasks and accessed many times a day for different reasons. It most likely has the capability to up and download files as well as send and receive email. PDA’s get viruses. For the same reasons you would think twice about saving your passwords on your PC or laptop, you should also exercise similar caution and reserve about keeping them on your PDA.

- Secondly, culture and convention. PDA’s are regularly shared among coworkers and friends. They are left around at the office, home or at client sites. Because of the nature of their use and physical size, PDA’s are not necessarily always in your control. The token was designed as an item of personal possession. Like your wallet or purse, it is under your control and has a singular purpose. It understood by all that it is something private. Where you would almost certainly be suspicious of someone attempting to “borrow” your wallet or token “just for a sec”, you probably wouldn’t think twice if they were to take a peak or wanting to borrow your PDA.

- Third, cryptographic strength. The token was designed from the ground up as a password manager. Kinetic circuitry actually senses your use of the unit. This aids the unit’s processor in the generation of strong passwords which thwart all known password cracking techniques including dictionary and brute force approaches. PDA’s do not possess or currently license such technology from Mandylion Labs. Accordingly, any password a PC or PDA program can calculate is considered inferior in strength because of its pseudo-random nature which can be predicted and easily defeated by various hacking techniques.

- Finally, cost and convenience. The token is an inexpensive device which is intuitively easy to use and addresses each of the hassles associated with passwords.

Q. How Many Passwords Can I Store With The Token?

A. The Mandylion Autoload Token can store and manage up to 50 passwords.

Q. What is a Login Record?

A. A Login Record is the term used to describe each password entry stored in the autoload token.

Each Login Record consists of three fields of data;

1. The identifying Name field of the Login Record; an
2. Account Number/User ID/Screen Name field; and
3. The Password itself (either input or created).

Q. What is a Password Schema?

A. A password’s schema is the term used to describe the set of variables used in a password’s construction.

These variables are the length (the number of characters in the password), the character set employed in each position of the password and expiration period of a password.

Q. What is the Personal Finger Authentication Pattern?

A. The personal finger authentication pattern is a combination of 5 unique keystrokes of the arrow keys. It is entered by the user to gain access to the Login Records contained on the unit. Your personal finger authentication pattern grants only you the access to the protected Login Records generated and stored by the unit. It is also used as part of the initial input into the unit’s random number generator.
Q. Why Does The Display Say Tampered?
A. If you ever accidentally enter the wrong personal finger authentication pattern or if unauthorized access to the unit is attempted, you will be discreetly warned the next time you gain access to the unit. The Main Display area will read Tampered. To clear this warning, simply press the enter key and continue to VIEW Mode.

Q. Why Does The Display Say “Locked Out”?
A. To further protect from unauthorized access, there are powerful lockout features incorporated into the token’s logic. If the wrong personal finger authentication pattern is attempted repeatedly, the unit will simply shut off for a specified period of time.

Q. Why Does The Display Say “Edit Lock”?
A. When the enter key is momentarily depressed while viewing any field, the Main Display area may read “EditLOCKED”. This signifies that the ability to edit that field has been limited by the enterprise.

Q. How Many Characters Can I Have In The Name Field Of The Login Record? Account Name Field? And The Password Field?
A. The autoload token is set to allow entry and display of up to 14 characters in each of the three fields of the Login Record. i.e. 14 characters for the login record name; 14 for the account / user ID / screen name and up to 14 characters in the password field.

Q. What is the “blinking black box” on the Display?
A. The autoload token allows for the entry of up to 14 characters in each of the three fields of the login record. The Main Display Area, however, only displays up to 10 characters of the field at a time.

The “blinking box” is a marker which signals the user that the field being viewed contains more than 10 characters. The display will display the first 9 characters of the field along with the “blinking box” marker in the 10th position. To view the remaining characters in the field, simply toggle the display by pressing either the left or right arrow keys. The display will then toggle between the primary display of the first 9 characters in the field and then in the secondary display, display up to the remaining 5 characters of the field for a total of 14 characters.

For positioning reference, especially with purely random strings, the secondary display repeats the last 4 characters of the primary display along with a “blinking box” separating the repeating characters from the remaining (up to) 5 characters to be displayed for the field.

Q. My employer blocks USB ports from being configured. How do I install?
A. Certain enterprise environments have instituted security policies which prevent unauthorized access to USB ports. Simply contact your security officer to gain access. Access is granted on an exception basis under the authority of Army Regulation 25-2 and DoD Policy 8500.
Q. In An Empty Login Record, The Display Shows “Blank #1”, Etc. In The Name Field; The Word “Empty” In The Account / UserID / Screen Name Field But Nothing In The Password Field. Why?

A. This is a security measure to ensure that you don’t actually mistake an empty Login Record as having a password in it before one can be entered or created for it.

Q. What is a Cryptographically Strong Password?

A. Generally speaking, a strong password is one which is designed to thwart compromise. The two most common password hacking techniques are dictionary style attacks and brute force attacks.

To thwart the dictionary attack, the password must be constructed of a purely random combination of the ASCII character set not previously available in any English or foreign language dictionary, data base or table. (Even the first letters of the lyrics to popular songs as well as output tables from known random number generators are now in hackers’ databases and easily available on the net).

To thwart the more formidable brute force attack, the password should be sufficiently long in length and regularly changed. An 8 character password comprised of a purely random combination of the full printable ASCII character set has the cryptographic key strength of a 56 bit encryption key. A 56 bit key is the DES encryption standard allowable for export by the United States Commerce Department.

Q. Why Won’t A Site Accept The Password I Generated?

A. Check with the site’s administrator or examine the site’s guide to passwords and access control. Unfortunately, certain sites restrict the number of characters and character sets a user may use in the construction of acceptable passwords. If that is the case either adjust the default schema or custom create a password schema for that site.

Q. What If The Battery Goes Dead?

A. The battery will last for approximately one year with normal use. When the charge falls to approximately 5% of the battery’s capacity, the Low Battery Indicator will light. Replace the battery as soon as possible. Don’t worry though if the battery goes completely dead. All entries are stored in permanent memory unaffected by battery life or loss of power.

To replace the battery, see the battery replacement section of this manual. The token uses a standard 3 volt “coin cell” style lithium battery (CR2032 or CR2025).

Q. What If I Cannot Recall My Personal Finger Authentication Pattern?

A. Because of the compensating factor that the device is small and portable enough to be in your physical possession and control, the Personal Finger Authentication Pattern was able to be designed as a simple easy pattern to remember. Much easier then even a simple password. Because of this, our experience is that it is rarely forgotten or mistaken by users. As a security measure, if the Personal Finger Authentication Pattern is forgotten, there is no other way to access the unit. No hidden back doors, no administrator or help desk intervention to retrieve its
contents. If you have forgotten your finger pattern, return your token to your administrator and have it reinitialized and new access codes generated.

**Q. What Does The DESTROY Choice In OPTIONS Mode Do If Selected?**

**A.** With this setting, the token’s logic will actually irretrievably erase and reset all Login Records, Passwords and entries if unauthorized access beyond the thresholds set are attempted.

The lockout features and tampered alarms, although strong, are merely deterrents to wrongful access and compromise of the device. They are part of the device's "defense in depth" strategy. When combined with the other features, controls and recommended use and possession of the device, they create a formidable barrier to wrongful access of the device. It is always theoretically possible to defeat a singular control, such as lockout, given enough time and persistence. Accordingly, relying on a single security feature in isolation of these other controls is not recommended. In high risk environments, Mandylion strongly recommends that users keep their tokens in their possession, remain vigilant as to possible signs of tampering and utilize the token as a memory aide via the use of offsets to the displayed password. (see the FAQ on how to use offsets)

**Q. Can the Mandylion autoload token / password management utility be configured and controlled by an administrator on behalf of the user? Alternatively, can it be self configured and administrated by the user themselves?**

**A.** Yes. Through an intuitive and secure Windows based interface and a common USB or serial port, each token can be customized and pre-configured on behalf of the user or class of users. For convenience, software is template based. All of the user’s logins, user ID’s and specific password requirements are entered onto the template then saved and downloaded into the device to which the user has been assigned.

With this new template approach, it is easy to configure a single unit or 5 thousand.

It’s as simple as a copy, paste and "print" exercise from one unit to the next. When provisioned with a token, all the user has to do is create their own finger pattern for access and they are done!

Unused login records can be set by the administrator to allow for the user’s personal use. Alternatively, a user can configure their own token from their own PC or a shared “kiosk” type station without the assistance of an administrator. Due to a unique lockout control, Login records set by the enterprise cannot be reconfigured or erased by the user. Alternatively, Login records set by the user cannot be reconfigured, erased or even accessed by the enterprise.
Q. Does the Mandylion autoload token / password management utility support Lotus Domino applications, iNotes and IBM Lotus Instant Messaging and Web Conferencing (Sametime) and Team WorkPlace (QuickPlace) logins.

A. The Mandylion autoload token / password management utility supports Lotus Domino applications including iNotes, Lotus IM and Web Conferencing and Team WorkPlace. The Mandylion solution works with any application or operating system which utilizes the durable password as its means for authenticating the user and granting it access privileges. Via the Configuration Management Software Module, user passwords can be specified by length, composition and renewal interval. Composition of each password can be specified down to the keyspace(position) within the passcode to be generated. Composition can be randomly drawn from the entire printable ASCII character set (base 94) or throttled to any or a combination of the following subsets of the printable ASCII character set:

- Upper Case Letters (base 26)
- Lower Case Letters (base 26)
- Upper and Lower Case Letters (base 52)
- Numbers (base 10)
- Special Characters (base 31)
- Any but Special Characters (base 63)
- National Character Set (base 3)(a mainframe legacy convention)

Q. Does the Mandylion autoload token / password management utility enable a single source for multiple logins?

A. The Mandylion solution includes a token provided to each user which allows the user to manage, secure and synchronize up to 50 individual login records.

Q. Can the Mandylion autoload token / password management utility synchronize group passwords?

A. The Mandylion solution allows for tokens to incrementally updated by login record for password composition and actual manual passwords. This allows for multiple tokens to share identical login records.

Q. Does the Mandylion autoload token / password management utility require client side software to be loaded and configuration controlled on each user’s system?

A. No. The Mandylion solution does not have any client side software. All logins are made by the user via their native applications and OS’s.

Q. What operating systems does the Configuration Management Utility software run under?

The Configuration Management Utility software runs on any Wintel platform including Microsoft Win32 (Windows 98, ME, NT 4.0, 2000, XP). The Mandylion solution, however, works with any application or operating system which utilizes the durable password as its means for authenticating the user and granting it access privileges. The Mandylion solution was specifically designed to work with and improve the vulnerabilities inherent in the MS LANMANv2 hash and its backward compatibility with previous versions of LANMAN. LANMAN is the central utility used in all MicrosoftOS products to authenticate users and secure their passcodes.
Q. What constraints can Mandylion autoload token / password management utility place on password composition?

A. The following options can be enabled or disabled by the Administrator in the creation of a password’s composition, by login record:

i. Minimum length; Maximum length;
ii. Password to be totally random; i.e. cannot contain the username or word;
iii. Can specify minimum representation of each ASCII character set;
iv. Password must contain a configurable number of numeric characters;
v. Password must contain a special character (from a customizable list)
vi. Password must contain at least one lowercase character;
vii. Password must contain at least one uppercase character;
viii. Password cannot be set to a previously used password;
ix. Password cannot contain any variation of the users name;
x. Password cannot can not be a dictionary word.

Q. Can the Mandylion autoload token / password management enable custom configuration of Expire On First Type Logins?

A. The Mandylion Configuration Management utility software sets the parameters for both the “bootstrap” or Expire on First Login password as well as the ongoing password policy for each login record. The administrator or user has the option of setting the Expire On First Login password to expire upon first use and automatically generate a new password for the user that complies with ongoing policy. Alternatively, the Expire On First Login password can be delayed to first policy change date or held static, as in the case of group or manual password login records.

Q. What expiration intervals can be set for each login record? Does a grace period for changing the password exist?

A. Password expiration intervals can be set and controlled by login record.

Intervals included in the standard configuration are:

- Upon First Use
- 30 Days
- 45 Days
- 60 Days
- 90 Days
- 180 Days
- One Year
- Two Years
- Never

Q. Does a grace period for changing an expired password exist? How do I coordinate password updates with other login records or with the Host password expiration interval?

Mandylion autoload token / password management utility allows for a “grace period” for password change to accommodate synchronization with other logins and applications as well as to temporarily delay password updates to a more convenient time to the user.

Q. Does the Mandylion Autoload Token provide security against unauthorized access to the token’s contents? Does it Enable strikeout limit functionality. Can the administrator set how many login attempts can be made before an unauthorized user “strikes out” with failed attempts?

A. The token possesses several tamper alarms, lockouts and limits on failed login attempts can be set and controlled by the administrator and/or the user. It employs both logical and physical controls to form a defense in depth approach to controlling the authorized use of the token.
Your Mandylion Token is of superior design and craftsmanship and should be treated with care. The suggestions below will help you to fulfill any warranty obligations and allow you to enjoy this product for many years.

When using your token, keep it out of small children’s’ reach. Keep it dry. Precipitation, humidity and liquids contain minerals that will corrode electronic circuits.

- **Do not** use or store it in dusty, dirty areas as its moving parts can be damaged.
- **Do not** store it in hot areas. High temperatures can shorten the life of electronic devices, damage batteries, and warp or melt certain plastics.
- **Do not** store it in cold areas. When the unit warms up (to its normal operating temperature), moisture can form inside, which may damage the units electronic circuit boards.
- **Do not** attempt to open it other than for battery maintenance. Non-expert handling of the device may damage it.
- **Do not** drop, knock or shake it. Rough handling can break internal circuit boards.
- **Do not** use harsh chemicals, cleaning solvents, or strong detergents to clean it. Wipe it with a soft cloth slightly dampened in a mild soap-and-water solution.
- **Do** familiarize yourself with all the access control and password management procedures and policies of the site or system you are using the unit with.
- **Do** take responsibility for your access control security. This product is only an aid in helping you achieve adequate protection.

If the unit is not working properly, take it to your nearest qualified service facility. The personnel there will assist you, and if necessary, arrange for service.

### General Information & Technical Data

<table>
<thead>
<tr>
<th>Weight</th>
<th>20g (&lt;1 oz.) with battery</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical Dimensions</td>
<td>65mm length (2.5 inches); 45mm width (1.5 inches); 10mm depth (3/8 inch).</td>
</tr>
<tr>
<td>Battery Type &amp; Voltage</td>
<td>User replaceable 3 volt “coin cell” style lithium battery (CR2032 or CR2025)</td>
</tr>
<tr>
<td>Operating Temperature</td>
<td>5°C to + 40°C (40°F to + 104°F)</td>
</tr>
</tbody>
</table>
Opening the Token Case
- 2 Simple Steps

Note of Caution: Although the Autoload Token is user and/or administrator serviceable, casually opening the token case is not recommended.

Physically, the token a simple design consisting of two halves; The front or top half (LCD/keypad side) where the token’s entire circuitry is permanently affixed and, the back or bottom half which contains the interface to the Policy Master Configuration Cradle. This cradle interface consists of 4 small pins which “float” in 4 ports that are molded into the back of the case. Care must be exercised in the opening of the token case only in order to prevent these pins from becoming lost during the battery replacement procedure. (see picture and inset).

To minimize the potential for the loss of these pins, please follow these two simple steps in opening the token case to replace the battery. (also please feel free to call or email Mandylion Labs if you require replacement pins).

Step #1. While making sure that the two halves of the case do not separate, use a small phillips-head screwdriver to loosen and remove the 3 screws that secure the two halves of the token.

DO NOT REMOVE THE BACK COVER OR SEPARATE THE HALVES OF THE TOKEN AT THIS POINT.

Step #2. Place token on a flat surface with LCD/keypad side face up. Carefully separate and remove the front half of the token case while keeping the back half stationary on the flat surface. While the token is disassembled, ensure that the 4 pins do not become lost.

Reassembly of the Token
To reconnect the two halves of the token, simply reverse the above procedure as follows:

#1. Place the back half (port side) of the token on a flat surface (external side down).

#2. Ensure that the 4 pins are fully inserted and floating in their ports (up to their flanges) on the inside back of the token case.

#3. Place the front half of the token (LCD/keypad side) case over the stationary back half and clasp together.

#4. While clasping the token halves together, reinsert the fasten the 3 screws with a small phillips-head screwdriver.

Battery Replacement
Snap out old battery from holder and replace battery with a 3 volt “coin cell” style lithium battery (CR2032 or CR2025).
Mandylion Research Labs, LLC ("MRL") warrants that the Mandylion Autoload Token ("Product") is free from defects in material and workmanship that result in Product failure during normal usage, according to the following terms and conditions:

1. The limited warranty for the Product extends for ONE (1) year beginning on the date of the purchase of the Product.
2. The limited warranty extends to the original purchaser of the Product ("Consumer") and is not assignable or transferable to any subsequent purchaser/end-user.
3. The limited warranty extends only to Consumers who purchase the Product in the United States.
4. During the limited warranty period, MRL will repair, or replace, at MRL's option, any defective parts, or any parts that will not properly operate for their intended use with new or factory rebuilt replacement items if such repair or replacement is needed because of product malfunction or failure during normal usage. No charge will be made to the Consumer for any such parts. MRL will also pay for the labor charges incurred by MRL in repairing or replacing the defective parts.
5. The limited warranty does not cover defects in appearance, cosmetic, decorative or structural items, including framing, and any non-operative parts. MRL's limit of liability under the limited warranty shall be the actual cash value of the Product at the time the Consumer returns the Product for repair, determined by the price paid by the Consumer for the Product less a reasonable amount for usage. MRL shall not be liable for any other losses or damages. These remedies are the Consumer's exclusive remedies for breach of warranty.
6. Upon request from MRL, the Consumer must prove the date of the original purchase of the Product by a dated bill of sale or dated itemized receipt.
7. The Consumer shall bear the cost of shipping the Product to MRL. MRL shall bear the cost of shipping the Product back to the Consumer after the completion of service under this limited warranty.
8. The Consumer shall have no coverage or benefits under this limited warranty if any of the following conditions are applicable:
   a) The Product has been subject to abnormal use, abnormal conditions, improper storage, exposure to moisture or dampness, unauthorized modifications, unauthorized connections, unauthorized repair, misuse, neglect, abuse, accident, alteration, improper installation, or other acts which are not the fault of MRL, including damage caused by shipping.
   b) Failure on the part of the Consumer to take ordinary steps towards the security of their access control.
   c) The Product has been damaged from external causes such as collision with an object, or from fire, flooding, sand, dirt, windstorm, lightning, earthquake or damage from exposure to weather conditions, an Act of God, or battery leakage, theft, or improper use of any electrical source, or damage caused by the connection to other products not recommended for interconnection by MRL.
   d) MRL was not advised by the Consumer in writing of the alleged defect or malfunction of the Product within fourteen (14) days after the expiration of the applicable limited warranty period.
   e) The Product serial number plate or the accessory data code has been removed, defaced or altered.
9. If a problem develops during the limited warranty period, the Consumer shall take the following step-by-step procedure: a) The Consumer shall return the Product to the place of purchase for repair or replacement processing. b) If “a” is not convenient because of distance (more than 50 miles) or for other good cause, the Consumer shall ship the Product prepaid and insured to a MRL facility. c) The Consumer shall include a return address, daytime phone number and/or fax number, complete description of the problem, proof of purchase and service agreement (if applicable). Expenses related to removing the Product from an installation are not covered under this limited warranty. d) The Consumer will be billed for any parts or labor charges not covered by this limited warranty. The Consumer will be responsible for any expenses related to reinstallation of the Product. e) MRL will repair or authorize the repair of the Product under the limited warranty within 30 days after receipt of the Product by MRL or an MRL authorized service center. If MRL cannot perform repair covered under this limited warranty within 30 days, or after a reasonable number of attempts to repair the same defect, MRL at its option, will provide a replacement Product or refund the purchase price of the Product less a reasonable amount for usage. f) If the Product is returned to MRL during the limited warranty period, but the problem with the Product is not covered under the terms and conditions of this limited warranty, the Consumer will be notified and given an estimate of the charges the Consumer must pay to have the Product repaired, with all shipping charges billed to the Consumer. If the estimate is refused, the Product will be returned freight collect. If the Product is returned to MRL after the expiration of the limited warranty period, MRL's normal service policies shall apply and the Consumer will be responsible for all shipping charges.
10. The Product consists of newly assembled equipment that may contain used components that have been reprocessed to allow machine compliance with Product performance and reliability specifications.
11. ANY IMPLIED WARRANTY OF MERCHANTABILITY, OR FITNESS FOR A PARTICULAR PURPOSE OR USE, SHALL BE LIMITED TO THE DURATION OF THE FOREGOING LIMITED WRITTEN WARRANTY. OTHERWISE, THE FOREGOING LIMITED WARRANTY IS THE CONSUMER'S SOLE AND EXCLUSIVE REMEDY AND IS IN LIEU OF ALL OTHER WARRANTIES, EXPRESS OR IMPLIED. MRL SHALL NOT BE LIABLE FOR SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES, INCLUDING BUT NOT LIMITED TO, LOSS OF ANTICIPATED BENEFITS OR PROFITS, LOSS OF SAVINGS OR REVENUE, PUNITIVE DAMAGES, LOSS OF USE OF THE PRODUCT OR ANY ASSOCIATED EQUIPMENT, COST OF CAPITAL, COST OF ANY SUBSTITUTE EQUIPMENT OR FACILITIES, DOWNTIME, THE CLAIMS OF ANY THIRD PARTIES, INCLUDING CUSTOMERS, AND INJURY TO PROPERTY, RESULTING FROM THE PURCHASE OR USE OF THE PRODUCT OR ARISING FROM BREACH OF THE WARRANTY, BREACH OF CONTRACT, NEGLIGENCE, STRICT TORT, OR ANY OTHER LEGAL OR EQUITABLE THEORY, EVEN IF MRL KNEW OF THE LIKELIHOOD OF SUCH DAMAGES. MRL SHALL NOT BE LIABLE FOR DELAY IN RENDERING SERVICE UNDER THE LIMITED WARRANTY, OR LOSS OF USE DURING THE PERIOD THAT THE PRODUCT IS BEING REPAIRED.
12. This is the entire warranty between MRL and the Consumer, and supersedes all prior and contemporaneous agreements or understandings, oral or written, and all communications relating to the Product, and no representation, promise or condition not contained herein shall modify these terms.
13. This limited warranty allocates the risk of failure of the Product between the Consumer and MRL. The allocation is recognized by the Consumer and is reflected in the purchase price of the Product.
14. Any action or lawsuit for breach of warranty must be commenced within eighteen (18) months following delivery of the Product.