Strong Authentication for Microsoft Windows Logon with

Powerful Authentication Management for Service Providers and Enterprises

Authentication Service Delivery Made EASY™
Copyright

Copyright © 2011. CRYPTOCard Inc. All rights reserved. The information contained herein is subject to change without notice. Proprietary Information of CRYPTOCard Inc.

Disclaimer

The information contained in this document may change without notice, and may have been altered or changed if you have received it from a source other than CRYPTOCard Inc. While every effort is made to ensure the accuracy of content offered on these pages, CRYPTOCard Inc. shall have no liability for errors, omissions or inadequacies in the content contained herein or for interpretations thereof.

Use of this information constitutes acceptance for use in an “AS IS” condition, without warranties of any kind, and any use of this information is at the user’s own risk.

No part of this documentation may be reproduced without the prior written permission of the copyright owner. CRYPTOCard Inc. disclaims all warranties, either expressed or implied, including the warranties of merchantability and fitness for a particular purpose. In no event shall CRYPTOCard Inc. be liable for any damages whatsoever, including direct, indirect, incidental, consequential or special damages, arising from the use or dissemination hereof, even if CRYPTOCard Inc. has been advised of the possibility of such damages. Some provinces, states or countries do not allow the exclusion or limitation of liability for consequential or incidental damages, so the foregoing limitation may not apply.

Links and addresses to Internet resources are inspected thoroughly prior to release, but the ever-changing nature of the Internet prevents CRYPTOCard Inc. from guaranteeing the content or existence of the resource. When possible, the reference contains alternate sites or keywords that could be used to acquire the information by other methods. If you find a broken or inappropriate link, please send an email with the topic name, link, and its behaviour to support@cryptocard.com.

The software described in this document is furnished under a license and may be used or copied only in accordance with the terms of the license.

Trademarks

BlackShield ID, CRYPTOCard and the CRYPTOCard logo are trademarks and/or registered trademarks of CRYPTOCard Corp. in Canada and/or other countries. All other goods and/or services mentioned are trademarks of their respective holders.
Contact Information

CRYPTOCard’s technical support specialists can provide assistance when planning and implementing CRYPTOCard in your network. In addition to aiding in the selection of the appropriate authentication products, CRYPTOCard can suggest deployment procedures that provide a smooth, simple transition from existing access control systems and a satisfying experience for network users. We can also help you leverage your existing network equipment and systems to maximize your return on investment.

CRYPTOCard works closely with channel partners to offer worldwide Technical Support services. If you purchased this product through a CRYPTOCard channel partner, please contact your partner directly for support needs.

To contact CRYPTOCard directly:

<table>
<thead>
<tr>
<th>United Kingdom</th>
<th>North America</th>
</tr>
</thead>
<tbody>
<tr>
<td>2430 The Quadrant, Aztec West, Almondsbury, Bristol, BS32 4AQ, U.K.</td>
<td>600-340 March Road, Kanata, Ontario, Canada K2K 2E4</td>
</tr>
<tr>
<td>Phone: +44 870 7077 700</td>
<td>Phone: +1 613 599 2441</td>
</tr>
<tr>
<td>Fax: +44 870 70770711</td>
<td>Fax: +1 613 599 2442</td>
</tr>
<tr>
<td><a href="mailto:support@cryptocard.com">support@cryptocard.com</a></td>
<td><a href="mailto:support@cryptocard.com">support@cryptocard.com</a></td>
</tr>
</tbody>
</table>

For information about obtaining a support contract, see our Support Web page at [http://www.cryptocard.com](http://www.cryptocard.com)
Introduction

By default Microsoft Windows logon requires that a user provide a correct user name and password to successfully logon. This document describes the steps necessary to augment this logon mechanism with strong authentication by adding a requirement to provide a one-time password generated by a CRYPTOCard token using the implementation instructions below.

Applicability

This integration guide is applicable to:

<table>
<thead>
<tr>
<th>Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication Server</td>
</tr>
<tr>
<td>Off-line Authentication Support</td>
</tr>
<tr>
<td>Supported Windows Versions</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Additional Software Components</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Supported Networking Environments</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Supported Architecture</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Network</td>
</tr>
<tr>
<td>Supported Tokens</td>
</tr>
<tr>
<td>Unsupported Tokens</td>
</tr>
<tr>
<td>Unsupported Tokens in Off-line Authentication Mode</td>
</tr>
</tbody>
</table>
Authentication Service Delivery Platform Compatibility

Publication History

<table>
<thead>
<tr>
<th>Date</th>
<th>Changes</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>January 26, 2010</td>
<td>Document created</td>
<td>1.0</td>
</tr>
<tr>
<td>April 9, 2010</td>
<td>Modified screenshots and text for management tool changes</td>
<td>1.1</td>
</tr>
<tr>
<td>September 24, 2010</td>
<td>Added additional information for GrIDsure tokens</td>
<td>1.2</td>
</tr>
</tbody>
</table>
Overview

The BlackShield ID agent for Microsoft® Windows® two-factor authentication solution is designed to help Microsoft enterprise customers ensure that valuable resources are accessible only by authorized users. It delivers a simplified and consistent user login experience, virtually eliminates help-desk calls related to password management, and helps organizations comply with regulatory requirements.

The use of two-factor authentication instead of just traditional static passwords to access a Windows environment is a necessary critical step for information security.

BlackShield Windows Logon – Domain Authentication

1. The user is presented with a BlackShield Windows Logon prompt then hit’s Ctrl + Alt + Del. User is presented with Username, OTP and Log on to.

2. The user enters their Username, OTP and, if applicable, selects their Log on to location. If the user is part of a Domain group authentication exception, the credentials are passed to Active Directory otherwise the Username and OTP are sent to the BlackShield ID Server for verification.

3. If the BlackShield credentials are valid, the user is prompted for their Microsoft password. If Microsoft password caching mode is enabled, the user is prompted for the Microsoft password only the first time they log on. Subsequently, the BlackShield ID Windows Logon agent will cache the Microsoft Windows password, furnishing the password as required.

4. If the Microsoft password is valid, the user logs on to the workstation.
BlackShield Windows Logon – Workgroup Authentication

1. The user is presented with a BlackShield Windows Logon prompt then hit’s Ctrl + Alt + Del. User is presented with Username and OTP.

2. The user enters their Username and OTP. If the user is part of a local group authentication exception, the credentials are passed to the local workstation otherwise the Username and OTP are sent to the BlackShield ID Server for verification.

3. If the BlackShield credentials are valid, the user is prompted for their Microsoft password. If Microsoft password caching mode is enabled, the user is prompted for the Microsoft password only the first time they log on. Subsequently, the BlackShield ID Windows Logon agent will cache the Microsoft Windows password, furnishing the password as required.

4. If the Microsoft password is valid, the user logs on to the workstation.
BlackShield Windows Logon – Off-line Authentication

1. The offline user is presented with a BlackShield Windows Logon prompt then hits Ctrl + Alt + Del. The offline user is presented with Username, OTP and Log on to location.

2. The offline user enters their Username, OTP and, if applicable, selects their Log on to location. If the offline user is part of a local group authentication exception, the credentials are passed to the local workstation otherwise the Username and OTP are verified by the off-line authentication one-time password store on the local workstation.

3. If the BlackShield credentials are valid, the user is prompted for their Microsoft password. If Microsoft password caching mode is enabled, the user is prompted for the Microsoft password only the first time they log on. Subsequently, the BlackShield ID Windows Logon agent will cache the Microsoft Windows password, furnishing the password as required.

4. If the Microsoft password is valid, the user logs on to the workstation.
Modes of Operation

There are two modes of operation for the BlackShield ID Windows Logon agent. The mode of operation is selected during installation but, if required, it can be modified afterwards. The modes of operation are:

<table>
<thead>
<tr>
<th>Mode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dual Password Mode</td>
<td>In Dual Password Mode, each user authenticates with a token-generated one-time password and then logs on with their Microsoft password. The user is prompted for the Microsoft password every time they log on.</td>
</tr>
<tr>
<td>Microsoft Password Caching Mode</td>
<td>In Microsoft Password Caching Mode, each user authenticates with a token-generated one-time password and then logs on with their Microsoft password. The user is prompted for the Microsoft password only the first time they log on. Subsequently, the BlackShield ID Windows Logon agent will cache the Microsoft Windows password, furnishing the password as required. However, the user will be prompted to supply a new password if/when Active Directory or the local workstation enforces a password-change policy.</td>
</tr>
</tbody>
</table>

Off-line Authentication

By default, the BlackShield ID Server supports off-line authentication; that is, the facility for a user to log on with a CRYPTOCard one-time password when there is no connection to the BlackShield ID Server. For details about disabling off-line authentication, see the BlackShield ID Server Administrator’s Guide.

The BlackShield Windows Logon agent permits end-user workstations that may be offline periodically to authenticate. The normal BlackShield Windows Logon agent authentication process requires that the user furnish a token-generated one-time password for transmission to the BlackShield ID Server. When offline, there is no communication with the BlackShield ID Server, only the local BlackShield Windows Logon agent. However, two-factor authentication is preserved: the user must have the token, and must know a PIN.

Off-line authentication is supported in both BlackShield Windows logon modes of operation (Dual Password and Microsoft Password Caching) with any account using the token types specified in the Error! Reference source not found. section.
The token can be enabled (i.e. using one-time passwords for logon) or disabled (i.e. using a BlackShield static password for logon). However, off-line authentication logon can only be done if the last logon before disconnecting from the network was done with a one-time password, the same applies if the user has been configured to use a BlackShield static password.

**Preparation and Prerequisites**

- Ensure that TCP port 80 or 443 is open between the BlackShield ID Windows Logon agent and the BlackShield ID Server.

- Administrative rights to the Windows system are required during installation of the BlackShield ID Windows Logon Agent.

- The BlackShield ID Windows Logon agent will attempt to download and install .Net 2.0 and MSXML 6 if not already present. Alternatively, if this is not possible, these packages can be found in the BlackShield distribution package.
Installation BlackShield ID Windows Logon Agent

1. Log on to the Windows system.

2. Locate and run one of the BlackShield ID installers below:
   - BlackShield ID Windows Logon Agent for XP-2003.exe (32 bit servers)
   - BlackShield ID Windows Logon Agent for XP-2003 x64.exe (64 bit servers)
   - BlackShield ID Windows Logon Agent for Vista-2008-7.exe (32 bit servers)
   - BlackShield ID Windows Logon Agent for Vista-2008-7 x64.exe (64 bit servers)

3. Accept the license agreement to continue with the installation.

4. Select the installation destination folder.

5. Enter the hostname or IP address of the primary BlackShield ID Server.

   Select “Connect using SSL” if BlackShield has been configured to accept incoming SSL connections.

   If available, tick the check box and add the hostname or IP address of a failover BlackShield ID server.

6. Select “Exempt Local and Domain Administrator groups from BlackShield ID Authentication” to allow administrators to login without providing CRYPTOCard credentials.

   Select a radio button to configure the BlackShield ID Logon Mode of operation.
BlackShield ID Windows Logon Agent Configuration Tool

The BlackShield ID Windows Logon Agent Configuration Tool allows for the customization of various options available within the BlackShield ID Windows Logon agent.

The Off-line, Policy, Communications, Appearance, Logging and Localization tabs are only available to users who are part of the local Administrators and Domain Administrators group. All other groups will be presented with the Off-line tab.

Off-line Tab

The Off-line tab deals primarily with end user off-line authentication settings. It displays the current amount of off-line authentication attempts, allows for the customization of the minimum warning notification threshold, the ability to manually replenish the off-line one-time password store and to test authentication requests against the BlackShield ID Server.

Off-line Authentication Settings

The BlackShield ID Windows Logon agent allows users to login to their workstations when the BlackShield ID server is not available.
Remaining off-line authentications: The amount of CRYPTOCard authentications available before the user must authenticate against the BlackShield ID Server or perform a manual replenish. The off-line authentications value is a global configuration setting configured within the Policy Admin, Authentication Policy section of the BlackShield ID Manager. Default value: 100.

Minimum off-line threshold: User will be displayed a warning to authenticate against the BlackShield ID Server or perform a manual replenish if this value if reached. Value may be between 5 and 99. Default value: 10.

Manually replenish

The off-line store is automatically replenished when a user returns and logs in to the corporate network but on the rare occasion, the off-line store may expire while the user is still at a remote location. The manually replenish option allows a user to refill their off-line authentication store remotely.

The user would follow these simple steps

1. The user makes a VPN connection to the corporate network.
2. The user launches the BlackShield ID Windows Logon Agent Configuration Tool.
3. User enters their CRYPTOCard credentials into the Passcode field then selects Connect.
4. The BlackShield ID Windows Logon Agent contacts the BlackShield ID Server, if the credentials supplied are valid, the off-line authentication is restored otherwise the user will receive a warning message to retry the authentication attempt.

Authentication Test

Allows Administrators to test authentication between the agent and the BlackShield ID Server.

Policy tab

The Policy tab allows CRYPTOCard authentication exclusions to be applied to the BlackShield Windows Logon agent.
Authentication Processing

Enable Agent: Turns the BlackShield ID Windows Logon agent on or off. Default value: Enabled.

Enable Emergency Password: Turns the emergency password feature on or off. Default value: Enabled.

The emergency password feature is an authentication method that enables an Administrator to authenticate to a user’s computer, as the user, without entering a CRYPTOCard one-time password. This only applies under two conditions:

1. The emergency password is enabled and the off-line authentication store is empty.
2. The emergency password is enabled and the Windows system is unable to communicate with the BlackShield ID server at the time of authentication.
Each user will have a unique emergency password found in the Secured Users tab of the BlackShield ID Manager.

This emergency password can be used until the workstation regains contact with the BlackShield ID Server at which point it will be randomized.

Enable Local/Domain Administrator strong authentication exemption: Allows the local and Domain Administrator group to be exempt from CRYPTOCard authentication during login. Default value is determined during installation of the agent.

Enable Microsoft password caching: Enables or disabled Microsoft password caching mode. Refer to the Modes of Operation section for more information.

Enable GrIDsure Tokens (2008, Vista and Windows 7 only): Enables or disabled the “Use GrIDsure Token” option displayed in the Windows Logon dialog prompts. This is required if users have been assigned GrIDsure tokens.

Credential Tile Filter (2008, Vista and Windows 7 only)

Only display CRYPTOCard credential Tile: All credential tiles presented to the user will enforce CRYPTOCard authentication.

Hide Microsoft credential Tile: The Microsoft credential tile is hidden from the user. Only the CRYPTOCard credential tiles and third party credential tiles are displayed.

Hide CRYPTOCard credential tile and show all available: Disables the CRYPTOCard credential tile and displays any third party and/or Microsoft credential tiles.

Group Authentication Exceptions

The group authentication exceptions section omits single and/or multiple local or domain groups from performing CRYPTOCard authentication. Only one group filter option is valid at any given time, it cannot overlap with another group authentication exception. Default value: Everyone must use CRYPTOCard.

Everyone must use CRYPTOCard: All users must perform CRYPTOCard authentication.

Only selected groups will bypass CRYPTOCard: All users are required to perform CRYPTOCard authentication except the Microsoft Group(s) defined.
Only selected groups must use CRYPTOCard: All users are not required to perform CRYPTOCard authentication except the Microsoft Group(s) defined.

From this location: Displays local or domain search results.

Enter the group name to select: Used in conjunction with Check Names or Show all. Allows searches for Microsoft groups.

Highlight already selected groups in search results: If a Microsoft Group has already been configured in the exception, it will appear as a highlighted result.

Communications Tab
This tab deals primarily with the connection options for the BlackShield ID Server.

Authentication Server Settings

Primary Server (IP:Port):
Used to configure the IP address / hostname of the primary BlackShield ID Server. Default is port 80. Alternatively Use SSL can also be selected. Default TCP port for SSL requests is 443.

Failover Server (Optional):
Used to configure the IP address / hostname of the failover BlackShield ID Server. Default is port 80. Alternatively Use SSL can also be selected. Default TCP port for SSL requests is 443.
Communication Timeout:

Sets the maximum timeout value for authentication requests sent to the BlackShield ID Server.

Attempt to return to primary Authentication Server every: Sets the Primary Authentication server retry interval. This setting only takes effect when the agent is using the Failover Server entry.

Agent Encryption Key File:

Used to specify the location of the BlackShield ID Agent Key File.

Server Status Check:

Performs a communication test to verify a connection to the BlackShield ID Server.

Appearance Tab

Allows for the customization of the logo that appears during authentication. The logo will vary depending on the operating system used.

Windows XP/2003: The custom logo must be a bitmap of 430 x 75 pixels. Solid white will be used as the transparent color if the image is smaller than 430 x 75 pixels.

Windows 2008/Vista/7: The custom log must be a bitmap of 110 x 110 pixels. Solid white will be used as the transparent color if the image is smaller than 110 x 110 pixels.

The restore option will revert to the default BlackShield logo for Windows XP/2003 or Windows 2008/Vista/7.
In Windows 2008, Vista and 7, a CRYPTOCard watermark will appear when a CRYPTOCard or custom logo is used.

Logging Tab

Logging Level:

Adjusts the logging level. For log levels, 1, 2 and 3, only the initial connection between the Agent and the Server and any failed connection attempts are logged. Default value is 3.

Log File location:

Specifies the location of the log files. The log files are rotated on a daily basis. The default location is: \Program Files\CRYPTOCard\BlackShield ID\Windows Logon\Gina\Logs.

Localization Tab

The settings in this tab represent the prompts and information messages provided by the BlackShield Windows Logon agent. These can be modified as necessary to improve usability. The LogonClient.ccl message file can also be manually modified outside of the configuration tool. The file can be found in the \Program Files\CRYPTOCard\BlackShield ID \Windows Logon\Gina\languages\en folder.
Migrating from CRYPTO-Logon 6.x

The following information is for CRYPTO-Server 6.x customers who are currently using the CRYPTO-Logon 6.x agent.

Architecture changes

- The CRYPTO-Logon for Domain Controller package is no longer required. The BlackShield Windows Logon package communicates directly with the BlackShield ID Server.
- The BlackShield Windows Logon package is supported in a Domain and/or Workgroup environment.
- The BlackShield Windows Logon package is not compatible with CRYPTO-Server 6.x.
- The network traffic used by the CRYPTOCard Windows logon agent has changed. The BlackShield Windows Logon agent uses TCP port 80 or 443. Previously, the CRYPTO-Logon 6.x used TCP port 5742.

Feature Changes

- CRYPTO-Logon 6.x Static Password Mode has been renamed Dual Password mode. CRYPTO-Logon 6.x Password Manager Mode has been renamed to Microsoft Password Caching Mode.
- Disconnected authentication has been renamed to Off-line authentication.
- Disconnected authentication is no longer enabled on a per token basis. Disconnected authentication is a global option, enabled by default, for all supported tokens specified in the Error! Reference source not found. section.
- The disconnected authentication warning message threshold is now customizable. Previously this was hard coded to 10. The warning message threshold value can be set between 5 and 99.
- Smart Card and USB tokens are not supported in the BlackShield Windows Logon package.

New Features

- The BlackShield Windows Logon agent includes a client-side configuration tool to allow customizations, which were previously only available via the registry.
- CRYPTOCard authentication exclusions can be added for specific Microsoft Groups.
- Allows the local and Domain Administrator groups to be exempt from CRYPTOCard authentication during login. This option is selectable during installation and can be disabled within the BlackShield Windows Logon configuration tool.
- Ability to control authentication credential tiles visible to users (Windows 2008/Vista/7 only).
- Silent install can be performed using the MSI installer package.
- The BlackShield Windows Logon agent supports custom logos.
- Various messages provided to the end user are now customizable.
- The BlackShield Windows Logon agent includes the ability for a user to manually replenish their off-line authentication information.
- An emergency password feature has been added. This feature is an authentication method that enables an Administrator to authenticate to a user’s computer, as the user, without entering a CRYPTOCard one-time password. Please consult the Authentication Processing section for more information.

**Upgrading to the BlackShield Windows Logon agent**

The BlackShield ID distribution package includes a 6.x migration tool that will copy all user, token and operator information from CRYPTO-Server 6.x into the BlackShield ID Server.

The default Inner Window value of 10 within the Policy Admin tab of the BlackShield ID Manager should be changed to 99 and the Outer Window value of 100 to 200. Modifying these settings will keep CRYPTOCard tokens in sync between each CRYPTOCard server as Windows workstations are migrated to the BlackShield Windows Logon package.

The CRYPTO-Logon 6.x Desktop client must be uninstalled prior to installing the BlackShield Windows Logon agent.

The 6.x CRYPTOCard software tools must be upgraded to the BlackShield Software Tools. Do not remove the 6.x CRYPTOCard software tools as this will remove any software tokens installed. During the installation of the BlackShield Software Tools any existing ST tokens will automatically be detected and imported. Once the tokens have been imported, the 6.x CRYPTOCard software tools package can be uninstalled. If a software token needs to be redeployed at a later date, an MP token must be issued to the user.

The CRYPTO-Logon for Domain Controller package should be the last component to uninstall after all workstations have been migrated to the BlackShield Windows Logon agent.
If Smart Card or UB tokens are being used, please contact your CRYPTOCard account manager for more information.

Advanced Configuration

BlackShield Windows Logon Silent install

The BlackShield Windows Logon msi installer package can be launched on the command line as follows:

```bash
msiexec /i "BlackShield ID Windows Logon Agent for XP-2003.msi" /quiet
```

to set options, the property name is used in name value pairs with spaces in between each pair.

For example to set the Primary BlackShield ID Server to 192.168.10.200 with SSL and enabled Microsoft Password Caching Mode you would run:

```bash
msiexec /i "BlackShield ID Windows Logon Agent for XP-2003.msi" /quiet TOKENVALIDATORLOCATION=192.168.10.200 USESSL=s LOGONMODE=1
```

The following is a list of options that can be specified. If the option is not specified, then it will get the default value, which is equivalent to just clicking Next, Next, Next through the installer.

<table>
<thead>
<tr>
<th>Description</th>
<th>Argument</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary BlackShield ID Server</td>
<td>TOKENVALDATORLOCATION</td>
<td>IP address or Hostname</td>
</tr>
<tr>
<td>Default Value: localhost</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enable SSL to Primary BlackShield ID</td>
<td>USESSL</td>
<td>S otherwise omit USESSL</td>
</tr>
<tr>
<td>Server</td>
<td>Default Value: Disabled</td>
<td></td>
</tr>
<tr>
<td>Secondary BlackShield ID Server</td>
<td>TOKENVALDATORLOCATION2</td>
<td>IP address or Hostname</td>
</tr>
<tr>
<td>Default Value: Disabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enable SSL to Secondary BlackShield ID Server</td>
<td>USESSL2</td>
<td>S otherwise omit USESSL2</td>
</tr>
<tr>
<td>Default Value: Disabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Exempt Admins</td>
<td>EXEMPTADMIN</td>
<td>1 for yes, 0 for no</td>
</tr>
<tr>
<td>Default Value: Enabled (1)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Logon Mode of Operation</td>
<td>LOGONMODE</td>
<td>0 for users will supply</td>
</tr>
</tbody>
</table>

Advanced Configuration
Microsoft Windows Logon with BlackShield

<table>
<thead>
<tr>
<th>Description</th>
<th>Argument</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default Value: Dual Logon (0)</td>
<td></td>
<td>both passwords each time</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 for Microsoft password caching</td>
</tr>
</tbody>
</table>

Remote users with a depleted off-line authentication store

The following steps should be taking if the emergency password is enabled and the off-line authentication store is empty resulting in the user being unable to login to their workstation:

1. The user contacts the BlackShield Administrator or operator.
2. The BlackShield Administrator or operator logs into the BlackShield ID Manager, finds the user in the Secured Users tab and makes note of the emergency password.
3. The BlackShield Administrator or operator provides the user with the emergency password.
4. The user logs in to their workstation using the emergency password.
5. The user makes a VPN connection into the network environment.
6. The user launches the BlackShield Windows Logon Configuration tool and performs a manual replenish with their CRYPTOCard credentials to restore their off-line authentication store. Do not attempt to replenish with the emergency password this will fail.
7. The user may now login while off-line with their CRYPTOCard credentials.

Remote users who have lost or forgotten their token

The following steps should be taking if the emergency password is enabled and the workstation is unable to communicate with the BlackShield ID server at the time of authentication:

1. The user contacts the BlackShield Administrator or operator.
2. The BlackShield Administrator or operator logs into the BlackShield ID Manager, finds the user in the Secured Users tab and makes note of the emergency password.
3. The BlackShield Administrator or operator provides the user with the emergency password.
4. The user logs in to their workstation using the emergency password.
5. The BlackShield Administrator or operator assigns the user with a new token or enables a BlackShield static password.
6. The user makes a VPN connection into the network environment.
7. The user launches the BlackShield Windows Logon Configuration tool and performs a manual replenish with the new token or BlackShield static password.
8. The user may now login while off-line with their CRYPTOCard credentials.

**Refining Administrator Group Exclusions**

During the installation of the BlackShield Windows Logon agent an option can be enabled to exempt the Local and Domain Administrators group from performing CRYPTOCard authentication. In certain cases, restrictions may only be needed for the local Administrator group or the Domain Administrators group rather than all Administrator groups. The following can be perform to achieve this goal:

1. During the installation of the BlackShield Windows Logon agent deselect “**Exempt Local and Domain Administrator groups from BlackShield ID Authentication**”.
2. Login to the BlackShield Windows Logon protected workstation with CRYPTOCard then Microsoft credentials.
3. Right click on the BlackShield Windows Logon Configuration tool and select “**Run As Administrator**”.
4. Select the Policy tab. In the Group Authentication Exceptions section, select "**Only selected groups will bypass CRYPTOCard**". Add the Administrator group(s) you'd like to exclude from CRYPTOCard authentication.
5. On Windows 2003/XP reboot the workstation for the setting to take effect otherwise logout then back in.

**Advanced Windows Login Settings**

**Do not display last user name**: Determines whether the name of the last user to log on to the computer is displayed in the Windows logon screen. This can be changed through the Local or Domain Policy.

1. Click Start, click Run, type mmc, and then click OK.
2. On the Console menu, click File, Add/Remove Snap-in.
3. Click Add.
4. Click the Group Policy snap-in, and then click Add.
5. Click the target Group Policy object (GPO). The default setting is the local computer. Click Browse to select other GPOs that are available on the network. Click Finish.
6. Click Close, and then click OK.
7. Expand the Computer Configuration node, the Windows Settings node, and the Security Settings node.
8. Expand the Local Policies node, and then click Security Options.
9. In the right pane, double-click "Interactive logon: the Do not display last user name" or "Do not display last user name" in logon screen entry.

10. Click Enabled.

11. Click OK.

12. Close the Group Policy console. Restart the workstation or server for the settings to take effect.

Configuring Num Lock settings:

The Num Lock setting can be controlled from the registry. If required, perform the following steps:

1. Click Start, click Run, and type regedit.

2. In the registry, open one of the following:

3. For a single user HKEY_CURRENT_USER\Control Panel\Keyboard

4. For all users KEY_USERS\.Default\Control Panel\Keyboard

5. The string value named "InitialKeyboardIndicators" control Numlock. These values are as follows:

6. Set it to 0 to set NumLock OFF

7. Set it to 2 to set NumLock ON

Further Information

For further information, please visit http://www.cryptocard.com