Strong Authentication for Microsoft OWA 2007/10 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
**Introduction**

By default Microsoft OWA logons 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>
</table>
| Authentication Server | BlackShield ID Server 2.4 or higher
| | BlackShield ID Server 2.6.573 or higher (GrIDsure support) |
| Network | TCP Port 80 or 443 |
| Supported Operating Systems | Microsoft Windows 2008
| | Microsoft Windows 2008 R2
| | Microsoft Windows Small Business Server 2008 |
| Supported Architecture | 64-bit |
| Supported Web Servers | IIS 7.0
| | IIS 7.5 |
| Supported Exchange Server Versions | Microsoft Exchange Server 2007
| | Microsoft Exchange Server 2010 |
| Supported Web Browsers | Internet Explorer 7, 8
| | Firefox 3.x |
| Additional Web Browsers Requirements | Cookies must be enabled
| | JavaScript must be enabled
| | ActiveX plug-ins (software token detection only) |

**Authentication Service Delivery Platform Compatibility**

![BlackShield Cloud](image)

![BlackShield Server](image)

**Publication History**

<table>
<thead>
<tr>
<th>Date</th>
<th>Changes</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>April 9, 2010</td>
<td>Document created</td>
<td>1.0</td>
</tr>
<tr>
<td>September 30, 2010</td>
<td>Minor updates</td>
<td>1.1</td>
</tr>
</tbody>
</table>
Overview

The BlackShield ID Agent for Outlook Web Access is designed to help Microsoft enterprise customers ensure that web based resources are accessible only by authorized users, whether working remotely or inside the firewall. It delivers a simplified and consistent user login experience and helps organizations comply with regulatory requirements.

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

BlackShield Outlook Web Access – Standard Authentication Mode (Hardware and Software)

1. The user enters the Outlook Web Access URL into their web browser.
2. The BlackShield agent examines the incoming request against its IP Range Exclusions/Inclusions list to determine if CRYPTOCard authentication can be ignored.
3. If IP address exclusion is detected, CRYPTOCard credentials are not required. The user authenticates using Microsoft credentials.
4. If IP address exclusion is not detected, a CRYPTOCard enabled login page appears.
5. If a software token is detected, the Outlook Web Access login page will display a Token, PIN, Microsoft Password and Microsoft Domain field. An option to toggle between hardware and software token mode will be available.
6. If a software token is not detected, the Outlook Web Access login page will display a Microsoft Username, Microsoft Password and OTP field.
7. The user enters their Microsoft and CRYPTOCard credentials into the login page. If both sets of credentials are valid, the user is presented with their mailbox otherwise, the attempt is
rejected.

BlackShield Outlook Web Access – Standard Authentication Mode (GrIDsure\SMS)

1. The user enters the Outlook Web Access URL into their web browser.
2. The BlackShield agent examines the incoming request against its IP Range Exclusions/Inclusions list to determine if CRYPTOCard authentication can be ignored.
3. If IP address exclusion is detected, CRYPTOCard credentials are not required. The user authenticates using Microsoft credentials.
4. If IP address exclusion is not detected, a CRYPTOCard enabled login page appears.
5. If a software token is detected, the Outlook Web Access login page will display a Token, PIN, Microsoft Password and Domain field. The option to toggle between hardware, software and GrIDsure\SMS token mode will be available.
6. If a software token is not detected, the Outlook Web Access login page will display a Microsoft Username, Microsoft Password and OTP field. The option to toggle between hardware and GrIDsure\SMS Challenge-response token mode will be available.
7. The user enters their Microsoft and CRYPTOCard credentials into the login page. If both sets of credentials are valid, the user is presented with their mailbox otherwise, the attempt is rejected.
8. In GrIDsure\SMS Challenge-response mode the user enters their Microsoft credentials into the login page. If the Microsoft credentials are valid the user is presented with a GrIDsure grid or provided with an OTP via SMS. If the CRYPTOCard credentials entered are valid, the user is presented with their mailbox otherwise, the attempt is rejected.
BlackShield Outlook Web Access - Split Authentication Mode

1. The user enters the Outlook Web Access URL into their web browser.
2. The BlackShield agent examines the incoming request against its IP Range Exclusions/Inclusions list to determine if CRYPTOCard authentication can be ignored.
3. If IP address exclusion is detected, CRYPTOCard credentials are not required. The user authenticates and logs into Outlook Web Access using their Microsoft credentials.
4. If IP address exclusion is not detected, the user is presented with a Microsoft Username, Microsoft Password field. If the Microsoft credentials are valid, the user is allowed to continue otherwise the attempt is rejected.
5. The BlackShield agent examines the Microsoft username against its Group Authentication Exceptions list to determine if CRYPTOCard authentication can be ignored.
6. If a group authentication exception is detected, CRYPTOCard credentials are not required. The user is presented with their mailbox.
7. If a group authentication exception is not detected, the BlackShield agent examines the Microsoft username against its GrIDsure and SMS authentication group list.
8. If a GrIDsure or SMS authentication group match is detected, the user is presented with their GrIDsure grid or provided with an OTP via SMS. If the CRYPTOCard credentials are valid, the user is presented with their mailbox otherwise, the attempt is rejected.
9. If a software token is detected, the Outlook Web Access login page will display a PIN field. The option to toggle between hardware and software mode will be available.
10. If a software token is not detected, the Outlook Web Access login page will display an OTP field.
11. The user enters their CRYPTOCard credentials into the login page. If the credentials are valid, the user is presented with their mailbox otherwise, the attempt is rejected.
Modes of Operation

There are two modes of operation for the BlackShield ID Agent for Outlook Web Access. By default, Split Authentication mode is enabled. The authentication mode can be modified after installation using the BlackShield Exchange Agent Configuration Tool.

The modes of operation are:

<table>
<thead>
<tr>
<th>Mode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standard Authentication Mode</td>
<td>Standard Authentication Mode enables a single stage login process. Microsoft and CRYPTOCard credentials must be entered into the Outlook Web Access login page.</td>
</tr>
<tr>
<td>Split Authentication Mode</td>
<td>Split Authentication Mode enables a two-stage login process. In the first stage, users provide their Microsoft credentials. In the second stage, users provide their CRYPTOCard credentials. This mode allows Administrators to control authentication dialogs based on Microsoft groups or token type (such as GrIDsure). This is the preferred mode when migrating from static to one-time passwords.</td>
</tr>
</tbody>
</table>
Preparation and Prerequisites

- Ensure that TCP port 80 or 443 is open between the BlackShield ID Agent for Outlook Web Access and the BlackShield ID Server.

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

Installing BlackShield ID Agent for Outlook Web Access

1. Log on to the Microsoft Exchange server.

2. Locate and run the BlackShield ID Agent for Exchange x64.exe installation package.

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 the version of Microsoft Exchange Server to protect.
BlackShield ID Exchange Agent Configuration Tool

The BlackShield ID Exchange agent configuration tool allows for the modification of various features available within the BlackShield ID Agent for Outlook Web Access.

Policy Tab
The Policy tab deals primarily with enabling the Outlook Web Access agent and defining the web site settings.

Authentication Processing

Enable Agent: Turns the BlackShield ID Agent for Outlook Web Access on or off. Default value: Disabled

Web Site

Web Site Name: Allows the selection of the Exchange Server web site. Default value: Default Web Site.

Microsoft OWA 2007/2010 with BlackShield

**Client IP Address Forwarding**

If selected, the remote client IP address will be sent to the BlackShield ID Server. Otherwise, the Web server’s IP Address will be used. Default value: Enabled.

**Authentication Methods Tab**

The Authentication Methods tab allows for the selection of the login authentication method and web page authentication layout presented to the user.

![Authentication Methods Tab](image)

**Authentication Methods**

**Standard Authentication Mode**: Standard Authentication Mode enables a single step login process. Microsoft and CRYPTOCard credentials must be entered into a single login page. Default value: Disabled.

Standard Authentication Mode provides the option to select one of two login templates:

**Hardware and Software Token Detection**: If a software token is detected, the login page will display a Token, PIN, Microsoft Password and Microsoft Domain field otherwise a Microsoft Username, Microsoft Password and OTP field is displayed. The option to toggle between Hardware and Software token mode will be available if a software token is detected on the local workstation.
Hardware, Software, GrIDsure and SMS Challenge Token Detection: If a software token is detected, the login page will display a Token, PIN, Microsoft Password and Microsoft Domain field. If required, a set of radio button options will allow the user to select a different token type. If no software token exists, the user will be presented with a Microsoft Username, Microsoft Password and OTP field along with an option to enable a GrIDsure\SMS Challenge login page.

Split Authentication Mode: Split Authentication Mode enables a two-stage login process. In the first stage, users provide their Microsoft credentials. In the second stage, users provide their CRYPTOCard credentials. Default value: Enabled.

This mode provides the following advantages over Standard Authentication Mode.

Microsoft group exclusions may be used to slowly migrate users from static passwords to a combination of static and one-time passwords.

Allows Administrators to specify via Microsoft Groups, users who have been provided with GrIDsure or SMS Challenge response tokens. This allows for a seamless login experience as the agent displays exactly what is required from the user.

GrIDsure Tab (Optional): Allows an Administrator to specify a Microsoft group, which contains CRYPTOCard users who have been assigned a GrIDsure token. When the agent detects a user within this group, it will automatically display a GrIDsure grid after they have provided valid Microsoft credentials.

SMS Challenge-Response Tab (Optional): Allows an Administrator to specify a Microsoft group, which contains CRYPTOCard users who have been assigned an SMS Challenge-response token. When the agent detects a user within the group, it will automatically provide them with a one-time password via SMS after they have provided valid Microsoft credentials.

Exceptions Tab
The Exceptions tab allows specific Microsoft groups or network traffic to bypass CRYPTOCard authentication. By default, all users are required to perform CRYPTOCard authentication unless otherwise defined by exclusion.

IP Range Exceptions/Inclusions

Allows an Administrator to define which network traffic requires CRYPTOCard authentication. By default, all networks are required to perform CRYPTOCard authentication.
**Group Authentication Exceptions**

Group authentication exceptions omit single and/or multiple 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.

The following group authentication exceptions are available:

- **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.
Adding a group authentication exception entry will display the following:

**From this location:** Select the location from which the results will be searched.

**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.

- **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.

- **Communication Timeout:** Sets the maximum timeout value for authentication requests sent to the BlackShield ID Server.

- **Agent Encryption Key File:** Used to specify the location of the BlackShield ID Agent Key File.
Authentication Test

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

Server Status Check

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

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. Log level 5 sets the agent in debug mode. Default value is 3.

Log File location:

Specifies the location of the log files. The log file is rotated on a daily basis. The default location is: \Program Files\CRYPTOCARD\BlackShield ID\Exchange\Log.

Localization Tab

The settings in this tab represent the prompts and information messages provided by the BlackShield ID Agent for Outlook Web Access. These can be modified as necessary to improve usability. The Messages.txt message file can also be manually modified outside of the configuration tool. This file can be found in the \Program Files\CRYPTOCARD\BlackShield ID \Exchange\LocalizedMessages folder.

Further Information

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