BlackShield ID™
Agent for Remote Web Workplace
Copyright

Copyright © 2010, CRYPTOCard All Rights Reserved. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form or by any means without the written permission of CRYPTOCard.

Trademarks

CRYPTOCard and the CRYPTOCard logo are registered trademarks of CRYPTOCard Inc. in the Canada and/or other countries. All other goods and/or services mentioned are trademarks of their respective companies.

License agreement

This software and the associated documentation are proprietary and confidential to CRYPTOCard, are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person.

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability.

This software is subject to change without notice and should not be construed as a commitment by CRYPTOCard.

Note on encryption technologies

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

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:

International Voice: +1-613-599-2441
North America Toll Free: 1-800-307-7042
support@cryptocard.com

Related Documentation


Publication History

<table>
<thead>
<tr>
<th>Date</th>
<th>Changes</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aug 27, 2010</td>
<td>Document created</td>
<td>1.0</td>
</tr>
</tbody>
</table>
## Table of Contents

Applicability .......................................................................................................................................................... 1

Overview ............................................................................................................................................................... 2

Authentication Modes ............................................................................................................................................... 2
  Remote Web Workplace - Standard Authentication Mode (Hardware and Software) ........................................ 3
  Remote Web Workplace - Standard Authentication Mode (Hardware, Software and GrIDsure/SMS) .......... 4
  Remote Web Workplace - Split Authentication Mode ..................................................................................... 5

Preparation and Prerequisites .................................................................................................................................. 6

Installing the BlackShield ID Agent for Remote Web Workplace ........................................................................... 6

Enabling the BlackShield ID Agent for Remote Web Workplace ............................................................................. 6

BlackShield ID Remote Web Workplace Agent Configuration Tool ......................................................................... 7
  Policy Tab .......................................................................................................................................................... 7
  Authentication Methods Tab ............................................................................................................................ 8
  Exceptions Tab ................................................................................................................................................. 9
  Communications Tab ........................................................................................................................................ 11
  Logging Tab .................................................................................................................................................... 12
  Localization Tab ............................................................................................................................................ 12

Troubleshooting .................................................................................................................................................... 12
  Error when launching the agent configuration tool ....................................................................................... 12
Applicability

This integration guide is applicable to:

<table>
<thead>
<tr>
<th>Summary</th>
<th></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 Small Business Server 2008 |
| Supported Architecture                       | 64-bit |
| Supported Web Servers                        | IIS 7.0 |
| 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) |
Overview

The BlackShield ID Agent for Remote Web Workplace 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 Remote Web Workplace is a necessary critical step for information security.

Authentication Modes

There are two login authentication modes available in the BlackShield ID Agent for Remote Web Workplace.

<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 Remote Web Workplace 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>

By default, Split Authentication mode is enabled. The authentication mode can be modified after installation using the BlackShield RWW Agent Configuration Tool.
Remote Web Workplace - Standard Authentication Mode (Hardware and Software)

1. The user enters the Remote Web Workplace 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 Remote Web Workplace login page will display a Token, PIN, Microsoft Password and Microsoft Domain field. An option to toggle between hardware and software token mode is available.
6. If a software token is not detected, the Remote Web Workplace 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 Remote Web Workplace portal otherwise, the attempt is rejected.
Remote Web Workplace - Standard Authentication Mode (Hardware, Software and GrIDsure/SMS)

1. The user enters the Remote Web Workplace 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 Remote Web Workplace login page will display a Token, PIN, Microsoft Password and Domain field. The option to toggle between hardware, software and GrIDsure/SMS token mode is available.
6. If a software token is not detected, the Remote Web Workplace 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 is 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 Remote Web Workplace portal 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 Remote Web Workplace portal otherwise, the attempt is rejected.
Remote Web Workplace - Split Authentication Mode

1. The user enters the Remote Web Workplace 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 the Remote Web Workplace portal 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 Remote Web Workplace portal.
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 Remote Web Workplace portal otherwise, the attempt is rejected.
9. If a software token is detected, the Remote Web Workplace login page will display the token name and a PIN field. The option to toggle between hardware and software mode is available.
10. If a software token is not detected, the Remote Web Workplace 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 Remote Web Workplace portal otherwise, the attempt is rejected.
Preparation and Prerequisites

- Ensure that users are able to login to Remote Web Workplace using their Microsoft credentials prior to deploying the agent.
- Ensure that TCP port 80 or 443 is open between the BlackShield ID Agent for Remote Web Workplace and the BlackShield ID Server.
- Administrative rights to the Windows system are required during installation and configuration of the BlackShield ID Remote Web Workplace Agent.

Installing the BlackShield ID Agent for Remote Web Workplace

1. Log on to the Microsoft Small Business Server as a user with administrative privileges.
2. Locate and run the BlackShield ID Agent for Remote Web Workplace x64.exe installation package.
3. Accept the license agreement.
4. 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.
5. Select the installation destination folder then proceed with the installation.

Enabling the BlackShield ID Agent for Remote Web Workplace

The following instructions are required for basic configuration of the agent. For more in-depth information on each setting, refer to the BlackShield ID Remote Web Workplace Agent Configuration Tool section.

1. Select Start, All Programs, CRYPTOCard, BlackShield ID Agent for Remote Web Workplace, RWW Agent Configuration.
2. In the Policy Tab under Web Site select the Browse button then choose SBS Web Applications. Verify the correct Remote Web Workplace User’s Group has been selected, by default this is Windows SBS Remote Web Workplace Users. Place a checkmark in Enable Agent. Enable any additional settings you require in this tab.
3. Select the Communications tab; verify the Authentication Server Settings reflect the location of the BlackShield ID server.
4. Verify that all other tabs meet your requirements.
5. Apply the settings. The IIS server will restart for the settings to take effect.
BlackShield ID Remote Web Workplace Agent Configuration Tool

The BlackShield ID Remote Web Workplace agent configuration tool allows for the modification of various features available within the BlackShield ID Agent for Remote Web Workplace.

Policy Tab

The Policy tab deals primarily with enabling the Remote Web Workplace agent and defining the web site settings.

Authentication Processing

Enable Agent: Turns the Remote Web Workplace agent on or off. Default value: Disabled

Session Timeout: Specifies the amount of time the user may remain idle before they are required to re-authenticate with their CRYPTOCard credentials. Default value: 10

Web Site

Web Site Name: Allows the selection of a Remote Web Workplace web site. Default value: Default Web Site.


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

**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, GirdSure 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 can be used 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 GirdSure/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.

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 server 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\RWW\Log\.

Localization Tab

The settings in this tab represent the prompts and information messages supplied by the agent. These can be modified as necessary to improve usability. The Messages.txt file can also be manually modified outside of the configuration tool. This file can be found in the \Program Files\CRYPTOCARD\BlackShield ID \RWW\LocalizedMessages folder.

Troubleshooting

Error when launching the agent configuration tool

Launching the RWW Configuration Tool generates a “System.Runtime.InteropServices.COMException (0x80070005): Access is Denied” message.

The configuration tool must be run as Administrator. Right click on the RWW Configuration Tool and select “Run as administrator”.