SafeNet Authentication Service

Configuration Guide

SAS Agent for Microsoft Remote Web Workplace

THE
DATA
PROTECTION
COMPANY

Document Information

Document Part Number	007-012694-001, Rev. A
Release Date	September 2014

Trademarks

All intellectual property is protected by copyright. All trademarks and product names used or referred to are the copyright of their respective owners. No part of this document may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, chemical, photocopy, recording, or otherwise, without the prior written permission of SafeNet, Inc.

Disclaimer

SafeNet makes no representations or warranties with respect to the contents of this document and specifically disclaims any implied warranties of merchantability or fitness for any particular purpose. Furthermore, SafeNet reserves the right to revise this publication and to make changes from time to time in the content hereof without the obligation upon SafeNet to notify any person or organization of any such revisions or changes.

We have attempted to make these documents complete, accurate, and useful, but we cannot guarantee them to be perfect. When we discover errors or omissions, or they are brought to our attention, we endeavor to correct them in succeeding releases of the product.

SafeNet invites constructive comments on the contents of this document. These comments, together with your personal and/or company details, should be sent to the address or email below.

Contact Method	Contact Information
Mail	SafeNet, Inc. 4690 Millennium Drive Belcamp, Maryland 21017, USA
Email	TechPubs@safenet-inc.com

Contents

Introduction

Third-Party Software Acknowledgement

This document is intended to help users of SafeNet products when working with third-party software, such as Microsoft Remote Web Workplace.

Material from third-party software is being used solely for the purpose of making instructions clear. Screen images and content obtained from third-party software will be acknowledged as such.

Applicability

This integration guide is applicable to the following:

Authentication Server	• SAS Server 2.4 or higher • SAS 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 SafeNet Authentication Service (SAS) 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.

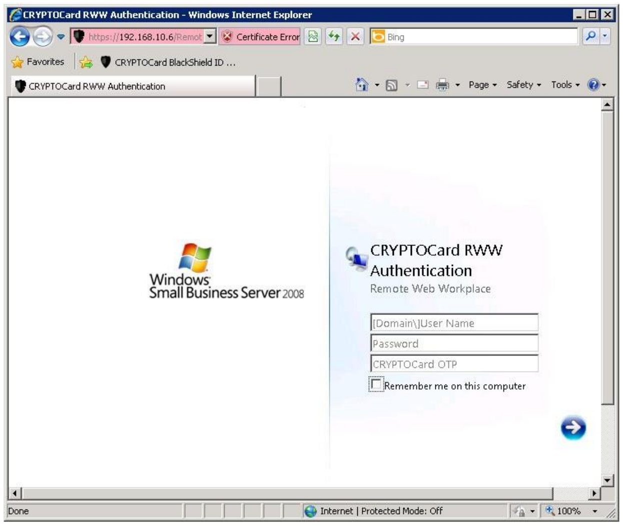
Authentication Modes

There are two login authentication modes available in the SAS Agent for Remote Web Workplace:

Mode	Description
Standard Authentication Mode	Standard Authentication Mode enables a single-stage login process. Microsoft and SafeNet credentials must be entered into the Remote Web Workplace 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 SafeNet 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 (OTPs).

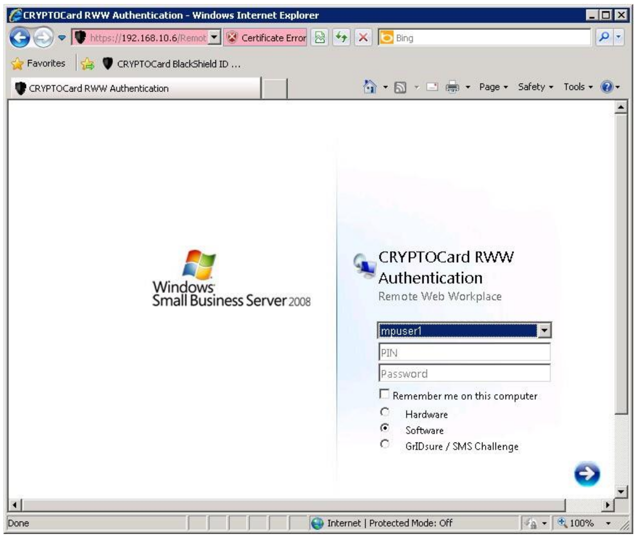
By default, **Split Authentication** mode is enabled. The authentication mode can be modified after installation using the SAS Agent Configuration Tool.

Standard Authentication Mode (Hardware and Software)


CRYPTOCard RWW Authentication - Windows Internet Explorer
https://192.168.10.6/Remot
Certificate Error
Bing
Favorites
CRYPTOCard BlackShield ID ...
CRYPTOCard RWW Authentication
Page
Safety
Tools
Windows Small Business Server 2008
Done
Internet | Protected Mode: Off
100%

CRYPTOCard RWW Authentication
Remote Web Workplace

[Domain\]User Name
Password
CRYPTOCard OTP
□ Remember me on this computer

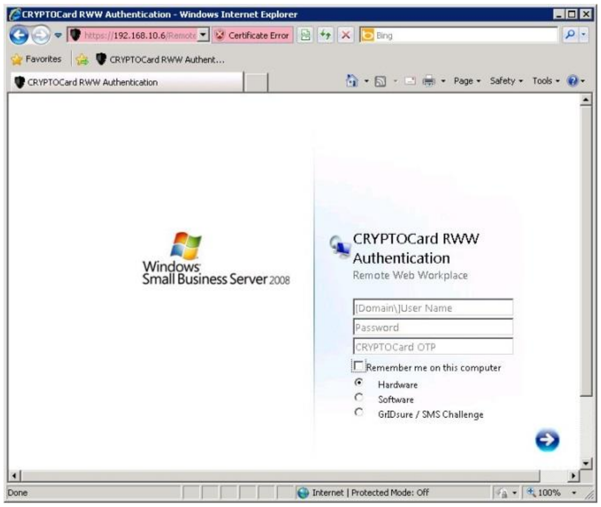

CRYPTOCard RWW Authentication - Windows Internet Explorer
https://192.168.10.6/Remot
Certificate Error
Bing
Favorites
CRYPTOCard BlackShield ID ...
CRYPTOCard RWW Authentication
Page
Safety
Tools
Windows Small Business Server 2008
Done
Internet | Protected Mode: Off
100%

CRYPTOCard RWW Authentication
Remote Web Workplace

mpuser1
PIN
Password
□ Remember me on this computer
○ Hardware
● Software
○ GrIDsure / SMS Challenge

1. The user enters the Remote Web Workplace URL into their web browser.
2. The SAS agent examines the incoming request against its **IP Range Exclusions/Inclusions** list to determine if SAS authentication can be ignored.
   - If IP address exclusion is detected, SAS credentials are not required. The user authenticates using Microsoft credentials.
   - If IP address exclusion is not detected, a SAS-enabled login page appears.
   - 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.
   - If a software token is not detected, the Remote Web Workplace login page will display a Microsoft **Username**, **Microsoft Password**, and **OTP** field.
3. The user enters their Microsoft and SAS 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.

Standard Authentication Mode (Hardware, Software and GrIDsure/SMS)


CRYPTOCard RWW Authentication - Windows Internet Explorer
https://192.168.10.6/Remote
Certificate Error
Bing
Favorites
CRYPTOCard RWW Authent...
CRYPTOCard RWW Authentication
Page
Safety
Tools
Windows Small Business Server 2008
Done
Internet | Protected Mode: Off
100%

CRYPTOCard RWW Authentication
Remote Web Workplace

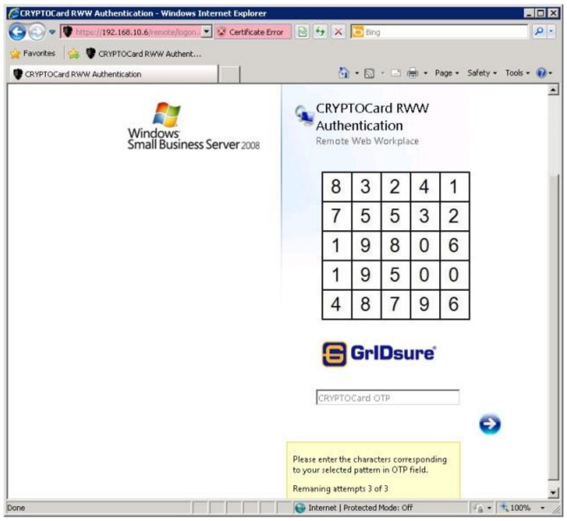
[Domain\]User Name

Password

CRYPTOCard OTP

□ Remember me on this computer

● Hardware
○ Software
○ GrIDsure / SMS Challenge


CRYPTOCard RWW Authentication - Windows Internet Explorer
https://192.168.10.6/remote/logon...
Certificate Error
Bing
Favorites
CRYPTOCard RWW Authent...
CRYPTOCard RWW Authentication
Page
Safety
Tools
Windows Small Business Server 2008
GrIDsure
Done
Internet | Protected Mode: Off
100%

CRYPTOCard RWW Authentication
Remote Web Workplace

8	3	2	4	1
7	5	5	3	2
1	9	8	0	6
1	9	5	0	0
4	8	7	9	6

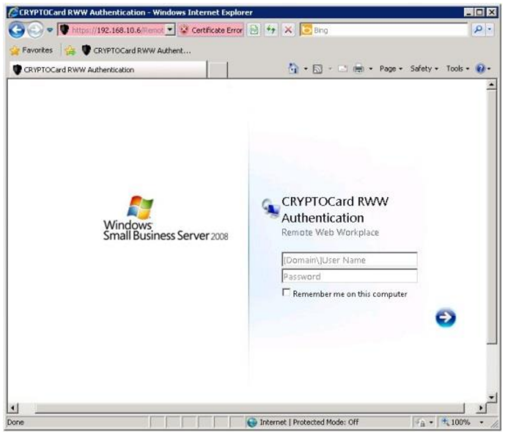
CRYPTOCard OTP

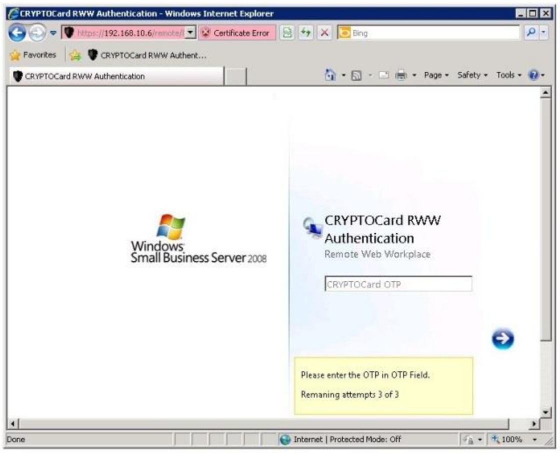
Please enter the characters corresponding to your selected pattern in OTP field.

Remaning attempts 3 of 3

1. The user enters the Remote Web Workplace URL into their web browser.
2. The SAS agent examines the incoming request against its **IP Range Exclusions/Inclusions** list to determine if SAS authentication can be ignored.
   - If IP address exclusion is detected, SAS credentials are not required. The user authenticates using Microsoft credentials.
   - If IP address exclusion is not detected, a SAS-enabled login page appears.
   - 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.
   - 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.
3. The user enters their Microsoft and SAS 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.
4. In GrIDsure/SMS challenge-response mode, the user enters their Microsoft credentials into the login page.
5. If the Microsoft credentials are valid, the user is presented with a GrIDsure grid or provided with an OTP via SMS. If the SAS 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


CRYPTOCard RWW Authentication - Windows Internet Explorer
https://192.168.10.6/Remot
Certificate Error
Bing
Favorites
CRYPTOCard RWW Authent...
CRYPTOCard RWW Authentication
Page
Safety
Tools
Windows Small Business Server 2008
CRYPTOCard RWW Authentication
Remote Web Workplace
[Domain]\User Name
Password
□ Remember me on this computer
Done
Internet | Protected Mode: Off
100%


CRYPTOCard RWW Authentication - Windows Internet Explorer
https://192.168.10.6/remote/
Certificate Error
Bing
Favorites
CRYPTOCard RWW Authent...
CRYPTOCard RWW Authentication
Page
Safety
Tools
Windows Small Business Server 2008
CRYPTOCard RWW Authentication
Remote Web Workplace
CRYPTOCard OTP
Done
Internet | Protected Mode: Off
100%

Please enter the OTP in OTP Field.

Remaning attempts 3 of 3

1. The user enters the Remote Web Workplace URL into their web browser.
2. The SAS agent examines the incoming request against its **IP Range Exclusions/Inclusions** list to determine if SAS authentication can be ignored.
   - If IP address exclusion is detected, SAS credentials are not required. The user authenticates and logs into the Remote Web Workplace portal using their Microsoft credentials.
   - If IP address exclusion is not detected, the user is presented with a **Microsoft Username** and **Password** fields. If the Microsoft credentials are valid, the user is allowed to continue; otherwise, the attempt is rejected.
3. The SAS agent examines the Microsoft username against its **Group Authentication Exceptions** list to determine if SAS authentication can be ignored.
   - If a group authentication exception is detected, SAS credentials are not required. The user is presented with their Remote Web Workplace portal.
   - If a group authentication exception is not detected, the SAS agent examines the Microsoft username against its GrIDsure and SMS authentication group list.
4. 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 SAS credentials are valid, the user is presented with their Remote Web Workplace portal otherwise, the attempt is rejected.
5. 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.
6. If a software token is not detected, the Remote Web Workplace login page will display an **OTP** field.
7. The user enters their SAS 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.

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 SAS Agent for Remote Web Workplace and the SAS server.
- Administrative rights to the Windows system are required during installation and configuration of the SAS Remote Web Workplace Agent.

Installing the SAS 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 SAS Agent for Remote Web Workplace **x64.exe** installation package.
3. Accept the license agreement.
4. Enter the hostname or IP address of the primary SAS server.
5. Select **Connect using SSL** if SAS has been configured to accept incoming SSL connections.
6. If available, select the check box and add the hostname or IP address of a failover SAS server.
7. Select the installation destination folder and proceed with the installation.

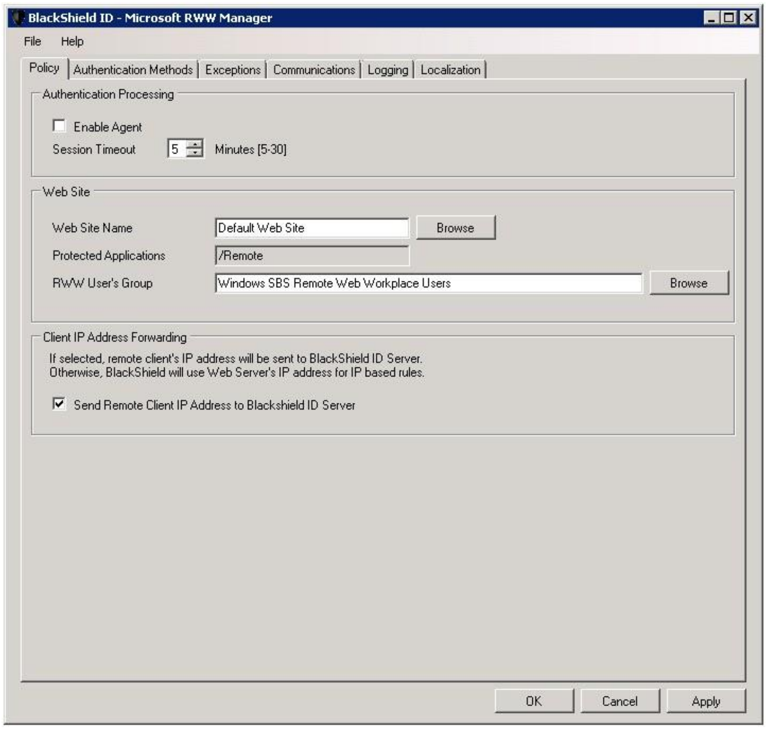
Enabling the SAS Agent for Remote Web Workplace

The following instructions are required for basic configuration of the agent. For detailed information on each setting, refer to the section “SAS Remote Web Workplace Agent Configuration Tool” on page 16.

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, and then choose **SBS Web Applications**.
3. Verify that the correct Remote Web Workplace User’s Group has been selected. By default, this is **Windows SBS Remote Web Workplace Users**. Select the **Enable Agent** option. Enable any additional settings you require in this tab.
4. Select the **Communications** tab. Verify that the **Authentication Server Settings** reflect the location of the SAS server.
5. Verify that all other tabs meet your requirements.
6. Apply the settings. The IIS server will restart for the settings to take effect.

SAS Remote Web Workplace Agent Configuration Tool

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



Authentication Processing

□ Enable Agent

Session Timeout 5 Minutes [5-30]

Web Site

Web Site Name: Default Web Site

Protected Applications: /Remote

RWW User's Group: Windows SBS Remote Web Workplace Users

Client IP Address Forwarding

If selected, remote client's IP address will be sent to BlackShield ID Server.
Otherwise, BlackShield will use Web Server's IP address for IP based rules.

☑ Send Remote Client IP Address to Blackshield ID Server

Policy Tab

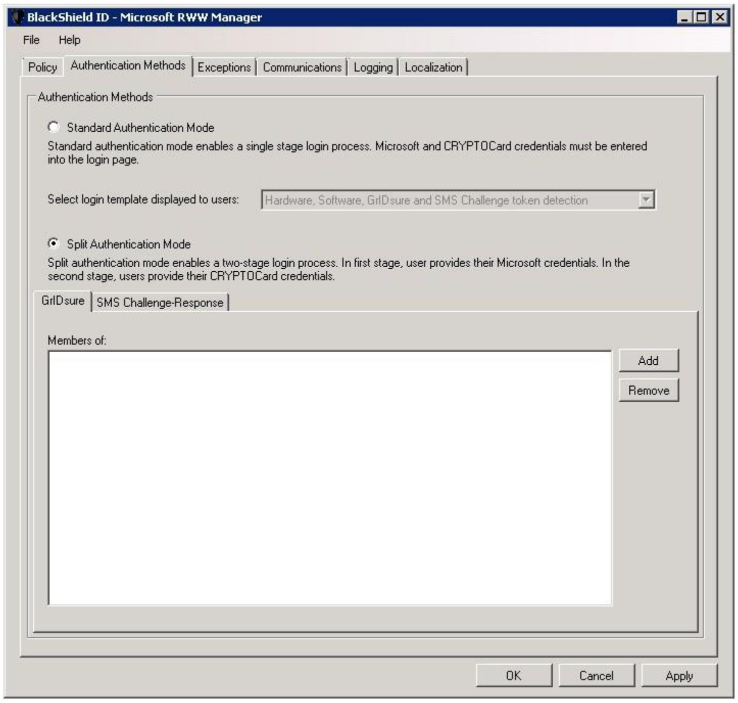
The **Policy** tab deals primarily with enabling the Remote Web Workplace agent and defining the web site settings.

- **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 SAS credentials. Default value: 10.
- **Web Site**
  - **Web Site Name:** Allows the selection of a Remote Web Workplace website. Default value: Default Web Site.
  - **Protected Applications:** Specifies the Remote Web Workplace directory. Default value: /Remote.
  - **RWW User's Group:** Specifies the default Microsoft Remote Web Workplace group users must belong to in order to access Remote Web Workplace. Default value: Windows SBS Remote Web Workplace Users.
- **Client IP Address Forwarding**

  If selected, the remote client IP address will be sent to the SAS 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 stage login process. Microsoft and CRYPTOCard credentials must be entered into the login page.

Select login template displayed to users: Hardware, Software, GrIDsure and SMS Challenge token detection

● Split Authentication Mode

Split authentication mode enables a two-stage login process. In first stage, user provides their Microsoft credentials. In the second stage, users provide their CRYPTOCard credentials.

Members of:

- **Authentication Methods**

- **Standard Authentication Mode:** Standard Authentication Mode enables a single-step login process. Microsoft and SAS 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 **Token**, **PIN**, and **Microsoft Password** and **Domain** fields; otherwise, **Microsoft Username** and **Password**, and **OTP** fields are 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 can be used to select a different token type. If no software token exists, the user will be presented with Microsoft **Username** and **Password**, and **OTP** fields 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 SAS 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.

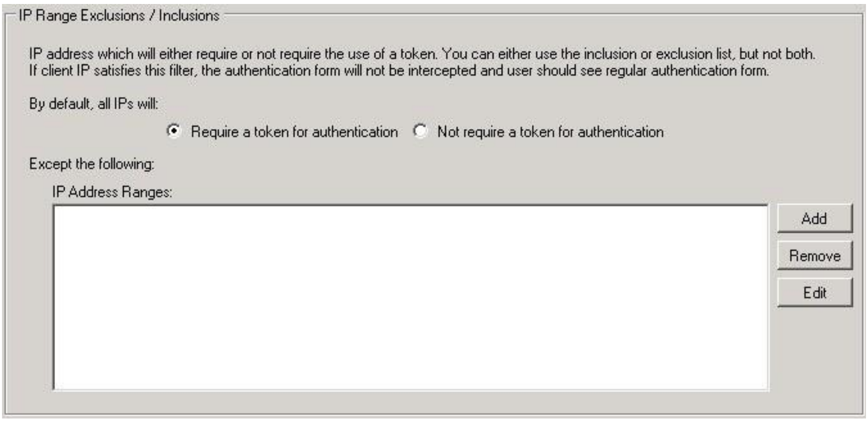
- **GrIDsure Tab (Optional):** Allows an administrator to specify a Microsoft group, which contains SAS users who have been assigned a GrIDsure token. When the agent detects a user within this group, it will automatically display a GrIDsure grid after they have provided valid Microsoft credentials.

- **SMS Challenge-Response Tab (Optional):** Allows an administrator to specify a Microsoft group, which contains SAS 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 SAS authentication. By default, all users are required to perform SAS authentication unless otherwise defined by exclusion.

- **IP Range Exceptions/Inclusions:** Allows an administrator to define which network traffic requires SAS authentication. By default, all networks are required to perform SAS authentication.



IP Range Exclusions / Inclusions

IP address which will either require or not require the use of a token. You can either use the inclusion or exclusion list, but not both.
If client IP satisfies this filter, the authentication form will not be intercepted and user should see regular authentication form.

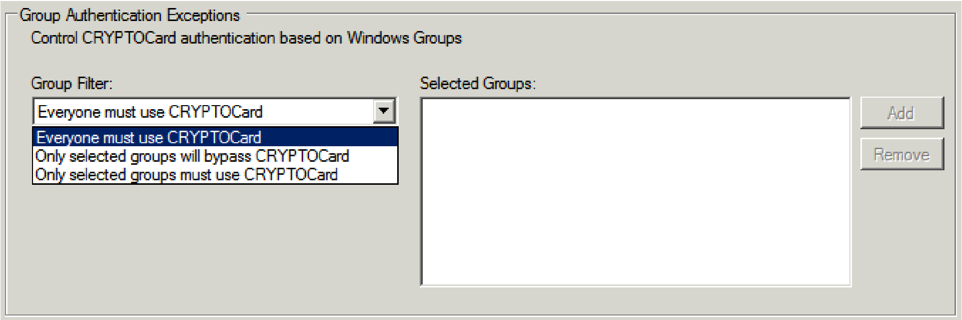
By default, all IPs will:

● Require a token for authentication ○ Not require a token for authentication

Except the following:

IP Address Ranges:

- **Group Authentication Exceptions:** Group authentication exceptions omit single and/or multiple domain groups from performing SAS 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 SAS.



Group Authentication Exceptions

Control CRYPTOCard authentication based on Windows Groups

Group Filter: Everyone must use CRYPTOCard

Everyone must use CRYPTOCard
Only selected groups will bypass CRYPTOCard
Only selected groups must use CRYPTOCard

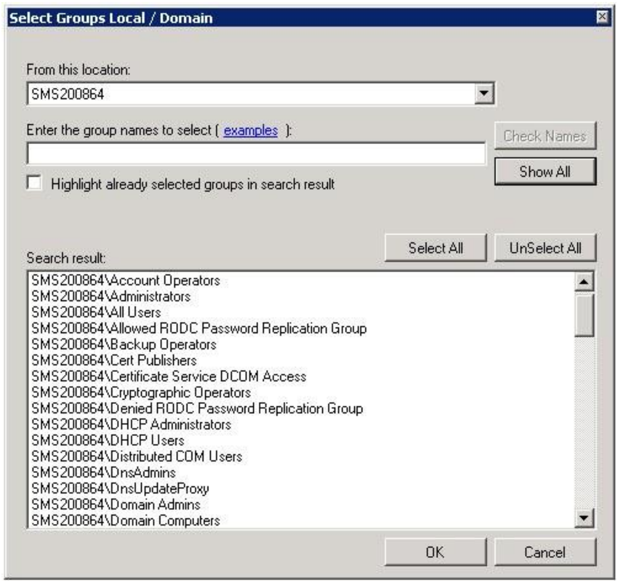
Selected Groups:

The following group authentication exceptions are available:

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



Select Groups Local / Domain

From this location: SMS200864

Enter the group names to select (examples):

□ Highlight already selected groups in search result

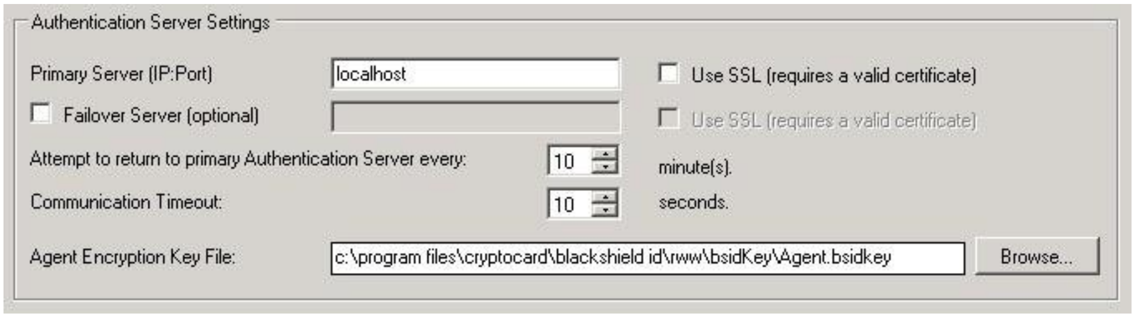
Search result:

SMS200864\Account Operators
SMS200864\Administrators
SMS200864\All Users
SMS200864\Allowed RODC Password Replication Group
SMS200864\Backup Operators
SMS200864\Cert Publishers
SMS200864\Certificate Service DCOM Access
SMS200864\Cryptographic Operators
SMS200864\Denied RODC Password Replication Group
SMS200864\DHCP Administrators
SMS200864\DHCP Users
SMS200864\Distributed COM Users
SMS200864\DnsAdmins
SMS200864\DnsUpdateProxy
SMS200864\Domain Admins
SMS200864\Domain Computers

Communications Tab

This tab deals primarily with the connection options for the SAS server.

- **Authentication Server Settings**



Authentication Server Settings

Primary Server (IP:Port): localhost ☐ Use SSL (requires a valid certificate)

☐ Failover Server (optional) ☐ Use SSL (requires a valid certificate)

Attempt to return to primary Authentication Server every: 10 minute(s).

Communication Timeout: 10 seconds.

Agent Encryption Key File: c:\program files\cryptocard\blackshield id\rww\bsidKey\Agent.bsidkey

  - **Primary Server (IP:Port):** Used to configure the IP address/hostname of the primary SAS server. Default is port 80. Alternatively, **Use SSL** can also be selected. The default TCP port for SSL requests is 443.
  - **Failover Server (Optional):** Used to configure the IP address/hostname of the failover SAS server. Default is port 80. Alternatively, **Use SSL** can also be selected. The 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** option.
  - **Communication Timeout:** Sets the maximum timeout value for authentication requests sent to the SAS server.
  - **Agent Encryption Key File:** Used to specify the location of the SAS Agent Key File.

- **Authentication Test:** Allows administrators to test authentication between the agent and the SAS server.
- **Server Status Check:** Performs a communication test to verify a connection to the SAS 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.

To correct this issue, run the RWW Configuration Tool as an administrator. To do so, right-click on the **RWW Configuration Tool** in the Start menu and select **Run as administrator**.

Support Contacts

If you encounter a problem while installing, registering, or operating this product, please make sure that you have read the documentation. If you cannot resolve the issue, contact your supplier or SafeNet Customer Support. SafeNet Customer Support operates 24 hours a day, 7 days a week. Your level of access to this service is governed by the support plan arrangements made between SafeNet and your organization. Please consult this support plan for further information about your entitlements, including the hours when phone support is available to you.

Table 1: Support Contacts

Contact Method	Contact Information	
Address	SafeNet, Inc. 4690 Millennium Drive Belcamp, Maryland 21017 USA	
Phone	United States	1-800-545-6608
	International	1-410-931-7520
Technical Support Customer Portal	https://serviceportal.safenet-inc.com Existing customers with a Technical Support Customer Portal account can log in to manage incidents, get the latest software upgrades, and access the SafeNet Knowledge Base.	