Implementation Guide for protecting
Microsoft Internet Security & Acceleration Server 2006 (ISA)
with
BlackShield ID
Copyright

Copyright © 2009, 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

BlackShield ID, BlackShield ID SBE and BlackShield ID Pro are either registered trademarks or trademarks of CRYPTOCard Inc. All other trademarks and registered trademarks are the property of their owners.

Additional Information, Assistance, or Comments

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>January 26, 2009</td>
<td>Document created</td>
<td>1.0</td>
</tr>
<tr>
<td>July 9, 2009</td>
<td>Copyright year updated</td>
<td>1.1</td>
</tr>
</tbody>
</table>
Table of Contents

Overview ......................................................................................................................... 1
Applicability .................................................................................................................. 1
Assumptions ................................................................................................................. 1
Operation ..................................................................................................................... 1
Preparation and Prerequisites ..................................................................................... 1
Configuration .............................................................................................................. 2
    Configuring ISA Server 2006 for Two-Factor authentication ............................ 2
Using the specified RADIUS Server with VPN configuration ................................. 4
Troubleshooting ......................................................................................................... 6
    Logging .................................................................................................................. 6
    Failed Logons ....................................................................................................... 6
Additional information .............................................................................................. 6
**Overview**
By default the Microsoft Internet Security & Acceleration Server 2006 requires that a user provide a correct user name and password to successfully logon to the VPN. 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 configuration instructions provided below.

**Applicability**
This integration guide is applicable to:

<table>
<thead>
<tr>
<th>Security Partner Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Partner</td>
</tr>
<tr>
<td>Product Name and Version</td>
</tr>
<tr>
<td>Protection Category</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CRYPTOCard Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication Server</td>
</tr>
<tr>
<td>Version</td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

**Assumptions**
BlackShield ID has been installed and configured and a “Test” user account can be selected in the Assignment Tab.

**Operation**
A RADIUS server is specified within the general server configuration section. The VPN connections are then configured to send authentication requests to the BlackShield ID RADIUS server. The BlackShield ID server then authenticates the provided credentials (User name and OTP), and either grants the user access or rejects the user access.

**Preparation and Prerequisites**
1. BlackShield ID agent for Microsoft Internet Authentication Service server (IAS) or Network Policy Server has been installed
2. The Microsoft ISA server must be a valid RADIUS client within your RADIUS server. This will allow RADIUS requests to be sent from Microsoft ISA 2006 to the RADIUS server.

**Configuration**

**Configuring ISA Server 2006 for Two-Factor authentication**

1. Launch the ISA Server Management tool.
2. Expand (Servername) > Configuration. Click on General.

3. Under "ISA Server Administration", click on “Specify RADIUS and LDAP Servers”
In the RADIUS Servers Tab, Click Add. The following window will appear.

Next click “Change…” to add a shared secret.

Next click “Change…” to add a shared secret.
Using the specified RADIUS Server with VPN configuration

1. In the ISA Server Management, click on Virtual Private Networks (VPN)

2. On the far right pane click on “Specify RADIUS Configuration”

3. In the RADIUS tab, place a check mark in “Use RADIUS Authentication” and “Use RADIUS for accounting (logging)”

4. Click “OK” when finished.
On the far right pane, under the VPN section, click “Enable VPN Client Access”
Troubleshooting

Logging

By default, Microsoft ISA server 2006 has the ability to show live logging information from its reporting features. This should be used as a primary log source to determine authentication issues. Upon requiring more information, the BlackShield ID snapshot tab should be used to determine authentication failure cause.

Failed Logons

<table>
<thead>
<tr>
<th>Symptom:</th>
<th>Authentication request is rejected by the VPN client.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Indication:</td>
<td>11/19/20 User Authentication Failure 31221234 192.168.21.1 Invalid PIN 08 Name on 5 20 e PM</td>
</tr>
<tr>
<td>Possible Causes:</td>
<td>An incorrect server side PIN is being used.</td>
</tr>
<tr>
<td>Solution:</td>
<td>Reset the server side PIN within the BlackShield ID console</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Symptom:</th>
<th>Authentication request is rejected by the VPN client.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Indication:</td>
<td>11/19/20 User Authentication Failure 31221234 192.168.21.1 Invalid authentication response 08 Name on 5 20</td>
</tr>
<tr>
<td>Possible Causes:</td>
<td>An invalid token code is being provided</td>
</tr>
<tr>
<td>Solution:</td>
<td>Verify the token code is being typed correctly. Verify the token code is being typed with all correct CaSiNg applied to all characters The token could be out of sync. Resync the token from within the console manager</td>
</tr>
</tbody>
</table>

Additional information

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