SafeNet Authentication Service

Integration Guide

Strong Authentication for Citrix Web Interface 4.6

Document Information

Document Part Number	007-012631-001, Rev A
Release Date	July 2009

Trademarks

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 Citrix Web Interface 4.6.

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.

Overview

By default, Citrix Web Interface logons requires that a user provide a correct user name and password to successfully log on. 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 SafeNet token using the SAS Agent for Citrix Web Interface.

Operation

The SAS Agent for Citrix Web Interface will place an additional field for one-time password input on the current Citrix Web Interface logon page. The user authenticates using their user name, static password and their SAS one-time password. The user is either granted or denied access based on the authentication request result.

Applicability

Security Partner Information	
Product Name	Citrix Web Interface 4.6
Vendor Site	http://www.citrix.com
Supported Client Software N/A	n/a
Authentication Method	SafeNet Authentication Service

Supported SAS Functionality	
SAS Authentication	RADIUS (PAP)
Authentication Mode	• One-time password • Challenge-response • BlackShield ID Pro static password
New PIN Mode	• User-changeable Alphanumeric 3-16 digit PIN • User-changeable Numeric 3-16 digit PIN

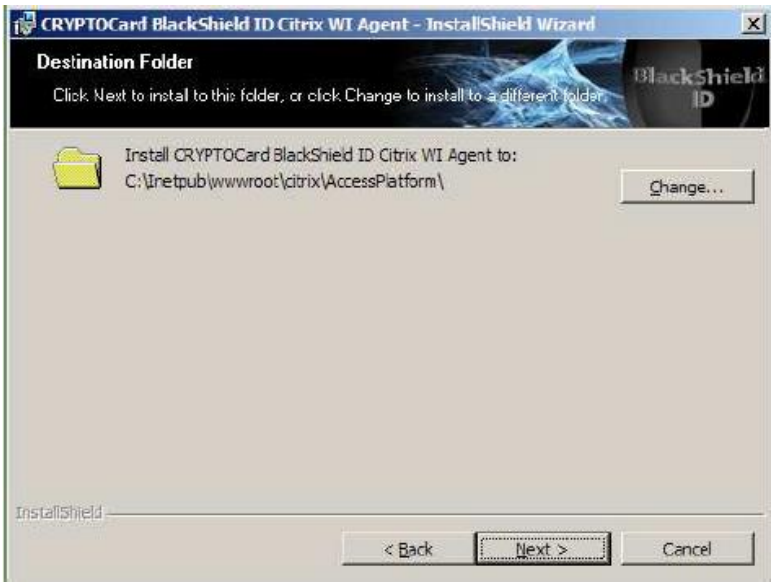
	• Server-changeable Alphanumeric 3-16 digit PIN • Server-changeable Numeric 3-16 digit PIN
Authentication Server	SAS
SAS Versions	All

Prerequisites

- Verify that a “Test” user account can successfully authenticate via the Citrix Web Interface 4.6 when the SAS agent is not installed.
- The Agent must be allowed to send TCP Port 80 or 443 network traffic to the SAS server. Ensure that the chosen port is open on any firewalls between the agent and the SAS server.

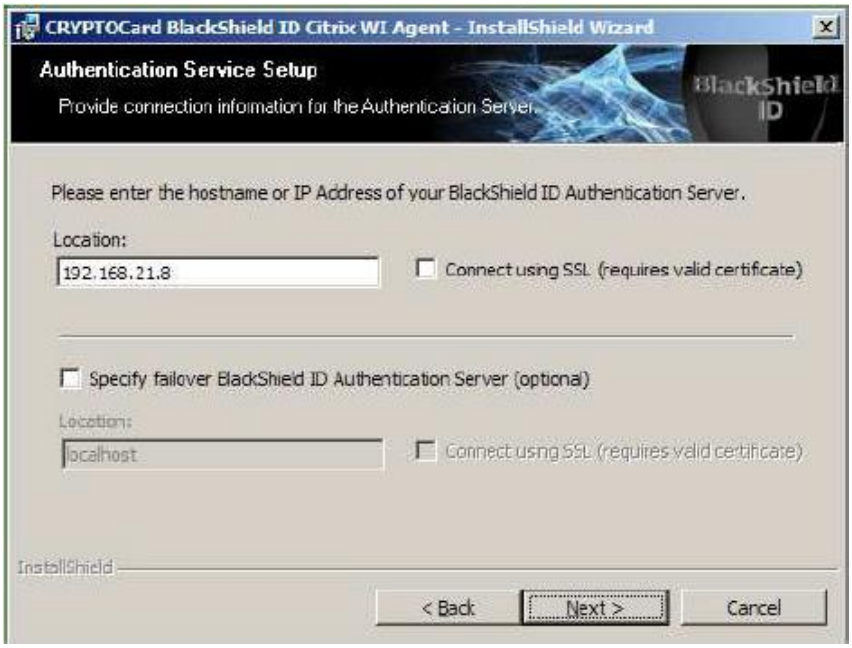
Installation

1. Run the Agent installer (“BlackShield ID Citrix Web Interface Agent.exe”) on the machine hosting Web Interface.
2. Accept or modify the Agent install location. Default: C:\Inetpub\wwwroot\citrix\AccessPlatform
3. Click **Next**.

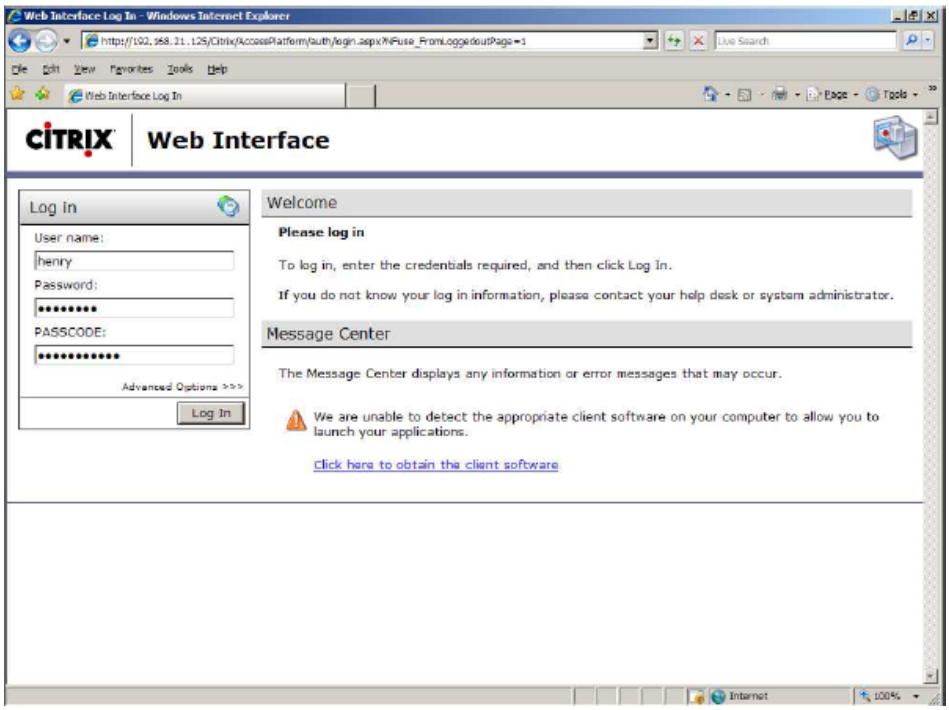


4. Enter in the hostname or IP Address of the SAS Server.

5. To configure failover, place a check mark in **Specify failover BlackShield ID Authentication Server** and then enter the hostname or IP address of the secondary server.



6. Using a web browser, navigate to the Citrix Web Interface 4.6 logon page. The web page now has an additional field called **PASSCODE**.



7. Perform a quick test by logging on with the **Test** account user name, password, and token one-time password. The users Web Interface page will be displayed when authentication succeeds.

Troubleshooting

Logging Level

By default, the Agent has the ability to log issues that arise when authenticating against SAS. To change the logging level, edit the following Registry key:

\HEKY_LOCAL_MACHINE\SOFTWARE\CRYPTOCard\AuthCitrix\Loglevel

By default the log level is set to 3. The log level runs from 1-5 where 1 is the lowest logging level and 5 is the most verbose logging. After changing the log level, IIS Admin service must be restarted for the new log level to take effect.

Log files are located in: \\Program Files\CRYPTOCard\BlackShield ID\Citrix Agent\Logs

Note that nothing is written to the log file for log levels 1, 2 or 3 unless the Agent is unable to connect to the server. All information gathered is from the SAS **Snapshot** tab in the SAS Manager.

Symptom	Login Failed
Indication	11/19/2008 12:36:49 PM Henry Authentication Failure 312191514 192.168.2.1 Invalid OTP
Possible Causes	The one-time password provided for the user is incorrect.
Solution	• Resync the token from the SAS Manager • Ensure the user is using the correct token and credentials

Symptom	Login Failed
Indication	11/19/2008 12:47:24 PM Henry Authentication Failure 312191514 192.168.2.1 Invalid PIN
Possible Causes	The PIN provided for the user is incorrect.
Solution	In SAS Manager, reset the PIN on the **Secured Users** tab.

Agent Upgrade

To upgrade this Agent, uninstall the current version and then run a newer version of the Agent installer. For more information, refer to the *SafeNet Authentication Service Administrator's Guide*.

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.

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.	