Trademarks

CRYPTOCard and the CRYPTOCard logo are registered trademarks of CRYPTOCard Corp. 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.

Third-party licenses

This product may include software developed by parties other than CRYPTOCard. The text of the license agreements applicable to third-party software in this product may be viewed in the \CRYPTOCard\BlackShield ID\Open Source Licenses folder of a default BlackShield ID installation.

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
Email: support@cryptocard.com


Go to the CRYPTOCard corporate web site for regional Customer Support telephone and fax numbers:
http://www.cryptocard.com
## Publication History

<table>
<thead>
<tr>
<th>Date</th>
<th>Changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>2009.07.24</td>
<td>Initial Release BlackShield ID v2.5</td>
</tr>
<tr>
<td>2009.10.16</td>
<td>Update for ICE (2.5i)</td>
</tr>
<tr>
<td>2010.01.26</td>
<td>Updated for BlackShield ID v2.6</td>
</tr>
<tr>
<td>2010.05.12</td>
<td>Update for MP token support for BlackBerry devices.</td>
</tr>
<tr>
<td>2010.09.13</td>
<td>Updated for BlackShield ID v2.7</td>
</tr>
</tbody>
</table>
Table of Contents

TRADEMARKS................................................................................................................................. I
LICENSE AGREEMENT........................................................................................................................ I
THIRD-PARTY LICENSES.................................................................................................................. I
NOTE ON ENCRYPTION TECHNOLOGIES.................................................................................... I
CONTACT INFORMATION................................................................................................................... I
PUBLICATION HISTORY..................................................................................................................... II
TABLE OF CONTENTS.......................................................................................................................... III

PREFACE ........................................................................................................................................... 1

BlackShield ID Documentation ...................................................................................................... 1

Related Documentation ............................................................................................................... 1

Before You Call Customer Support ............................................................................................ 1

CHAPTER 1 – ABOUT THIS GUIDE ................................................................................................. 3

New in BlackShield ID v2.7........................................................................................................ 3

CHAPTER 2 – INTRODUCING BLACKSHIELD ID.............................................................................. 4

BlackShield ID Architecture...................................................................................................... 4

User Sources ............................................................................................................................... 4

Multiple LDAP User Sources .................................................................................................. 5

RADIUS ................................................................................................................................ 5

Agents ........................................................................................................................................... 5

Authentication API.................................................................................................................... 6

Basic Authentication.................................................................................................................. 6

Advanced Authentication ........................................................................................................ 7
Source Agent and IP .......................................................................................................................... 8
Multiple User Data Sources .................................................................................................................. 9
PreAuthentication Rules ....................................................................................................................... 9
Security Policy ....................................................................................................................................... 10

Provisioning ........................................................................................................................................ 10
Automated Bulk Provisioning ................................................................................................................ 10
Self-enrollment .................................................................................................................................... 11
Customization and Internationalization ............................................................................................. 11

CHAPTER 3 – TOKENS .......................................................................................................................... 12
CRYPTOCARD Tokens and Two-factor Authentication ......................................................................... 12
Token Selection .................................................................................................................................... 13
Battery Replacement ............................................................................................................................ 15
Privacy, Data Protection and Token Initialization ............................................................................... 15
Factory Pre-programmed Tokens ........................................................................................................ 16
Unprogrammed Tokens ....................................................................................................................... 16
Software Tokens .................................................................................................................................. 17
Components ........................................................................................................................................ 17

CHAPTER 4 – GETTING STARTED ........................................................................................................ 18
Supported Operating Systems ............................................................................................................. 18
Supported Databases ........................................................................................................................... 19
Supported LDAP Servers ..................................................................................................................... 19
Architecture ......................................................................................................................................... 19
Supported Internet Protocols ............................................................................................................... 19
Software Requirements ....................................................................................................................... 19
Hardware Requirements ...................................................................................................................... 20
Other Requirements ......................................................................................................... 20
Virtualization ..................................................................................................................... 20
Internal Database .............................................................................................................. 21
LDAP External User Sources .............................................................................................. 21
Supported Browsers ......................................................................................................... 22
Ports .................................................................................................................................. 23
Agents ............................................................................................................................... 23
Maintaining Accurate Time Settings .................................................................................. 24
Installation Types .............................................................................................................. 24
  Small Business Server Deployments ............................................................................... 25
  Small, Single-Site Deployments .................................................................................... 25
  Medium Site Deployments ............................................................................................ 26
  Large Deployments ...................................................................................................... 27
What you need to begin ................................................................................................... 27
Standard Installation ....................................................................................................... 28
Custom Installation .......................................................................................................... 28

CHAPTER 5 – INSTALLING BLACKSHIELD ID SERVER AND RADIUS...................................... 29
Installation BlackShield ID Server .................................................................................. 29
Installing RADIUS .......................................................................................................... 30
  Preparation and Prerequisites ....................................................................................... 31
  Installation ..................................................................................................................... 31
Configure Microsoft IAS for RADIUS Client(s).............................................................. 32
  Installation BlackShield ID Agent for IAS .................................................................... 33
    Configure IAS to use BlackShield ID Agent ............................................................... 34
    Create a Remote Access Policy ............................................................................... 34
    Create a Connection Request Policy ...................................................................... 36
Configure Microsoft NPS for RADIUS Client(s) ................................................................. 38
  Installation BlackShield ID Agent for NPS ........................................................................... 39
  Configure NPS to use BlackShield ID Agent......................................................................... 40
    Creating a Connection Request Policy .................................................................................. 40

Configure the BlackShield ID Agent for IAS / NPS............................................................. 41
  NPS/IAS Settings .................................................................................................................... 42
  Communication Settings ....................................................................................................... 42
  Authentication Test................................................................................................................ 43
  Logging .................................................................................................................................... 43
  Localization ............................................................................................................................. 44

CHAPTER 6 – CONFIGURING BLACKSHIELD ID ........................................................................ 45

Basic BlackShield ID Configuration ................................................................................... 45

Actions Group ................................................................................................................... 46

System Setting: SQL .......................................................................................................... 47

Alternative Database Configuration ....................................................................................... 48
  MySQL 5.x Database Configuration ...................................................................................... 49
  MS-SQL Database Configuration .......................................................................................... 51
  Oracle Database Configuration ............................................................................................. 53

Licenses ................................................................................................................................... 54

System Settings: Users........................................................................................................ 54
  LDAP User Source Configuration .......................................................................................... 55
    Custom Schema Support .................................................................................................... 56
  Internal SQL User Source Configuration .............................................................................. 57
  MySQL User Data Source ..................................................................................................... 59
  MS-SQL User Data Source ................................................................................................... 61
  Oracle User Data Source ...................................................................................................... 63

Advanced Configuration - System Admin Tab .................................................................. 64
  Mail Settings ....................................................................................................................... 64
    Configure Mail Settings ................................................................................................. 64
Passcode Policy Group................................................................. 81
Operation Policy Group .............................................................. 82
PIN Policy Group........................................................................... 83
Third Party Authentication Options............................................ 84
Synchronization.............................................................................. 84
Inner OTP synchronization window size ....................................... 85
Outer OTP synchronization window size ....................................... 85
Authentication Thresholds Group .................................................. 85
Account Lock threshold ............................................................... 85
Alert Operator on Account Lockout ............................................. 86
Alert User on Account Lockout.................................................. 86
Account Lock Duration ............................................................... 86
Alert Operator on Account Unlock ............................................. 86
Alert User on Account Lockout.................................................. 86
Server-side PIN Policy.................................................................... 86
Change PIN on first use required ............................................... 87
Force Random PINs ...................................................................... 87
Minimum Length .......................................................................... 87
Maximum Length ......................................................................... 87
Minimum Complexity .................................................................... 87
Change Frequency ....................................................................... 88
Random PIN Length ...................................................................... 88
PIN Change Exclusion List .......................................................... 88
Temporary Password Policy......................................................... 88
Temporary password Allowed..................................................... 89
Change Password on first use required ....................................... 89
Minimum Length .......................................................................... 89
Maximum Length ......................................................................... 89
Minimum Complexity .................................................................... 89
Change Frequency ....................................................................... 90
Force Random Passwords............................................................ 90
Force Maximum Lifetime ........................................................... 90
Authentication Policy ..................................................................... 90
Restrictions Group........................................................................................................................... 91
Token File Creation .......................................................................................................................... 91
Allowed Targets Settings (Settings) ................................................................................................. 91
  General Settings .............................................................................................................................. 92
  Settings ........................................................................................................................................ 92
  MP Token Targets .......................................................................................................................... 92
Allowed Targets Settings (Devices)................................................................................................... 93
  New Device .................................................................................................................................. 93
Token File Location Group................................................................................................................ 94
Third Party Authentication Options .................................................................................................. 94
  Allow trivial PIP’s: ......................................................................................................................... 94
  Use Numbers ............................................................................................................................... 94
  Use special symbols/characters ..................................................................................................... 94
  Use uppercase letters .................................................................................................................... 94
  Use lowercase letters .................................................................................................................... 94
Assignment Tab............................................................................................................................... 95
  Assignment Search / Users: Containers ....................................................................................... 96
  Assignment Search / Users: Assignment Search Group ............................................................... 97
  User ............................................................................................................................................ 97
  User Detail .................................................................................................................................. 98
  Assigned Tokens Group ................................................................................................................ 98
  User Mgmt Group ......................................................................................................................... 99
  Add a User to the internal SQL User Source ............................................................................. 99
  Edit or Remove a User from the Internal SQL user data source ................................................ 100
Overview of Token Management ................................................................................................... 100
  Import ....................................................................................................................................... 100
  Initialization ................................................................................................................................. 100
  Create ....................................................................................................................................... 100
Import Tokens ................................................................................................................................. 101
Initialize Tokens ............................................................................................................................. 101
  Preparing the KT series token for Initialization ....................................................................... 102
  Preparing the RB series token for Initialization ....................................................................... 103
Software tokens .............................................................................................................. 104
  Create ........................................................................................................................................... 104
  MP Token ...................................................................................................................................... 105
  SMS Token .................................................................................................................................... 105

Token Search ................................................................................................................... 105

Token Management ........................................................................................................ 107

Issuing Tokens ................................................................................................................. 109
  Assign Token Function ................................................................................................................... 109
    Assign Hardware Tokens .............................................................................................................. 110
    Assign Software Tokens ........................................................................................................... 110
  Hard Drive Installation ........................................................................................................... 110
  BlackBerry Installation ......................................................................................................... 111
  IronKey Enterprise Secure Flash Driver Installation ................................................................ 111
  SMS/OTP Zero footprint tokens ............................................................................................. 111
  Example MP Software Token Assignment ..................................................................................... 112

Temporary Passwords ..................................................................................................... 113
  Temporary Password Assignment ................................................................................................. 114

Self-Enroll Function ......................................................................................................... 116
  Self-enroll hardware tokens ........................................................................................................ 116
  Self-enroll MP software tokens ................................................................................................. 116
    Hard Drive Installation ........................................................................................................... 117
    IronKey Enterprise Secure Flash Driver Installation ................................................................ 117
  Example MP Software Token Self-Enrollment ............................................................................... 117

Access Restrictions ........................................................................................................ 118

Rule-based Provisioning ................................................................................................. 120
  Configure Rule-based Provisioning ................................................................................................ 120

Command Line Interface (CLI) Provisioning .................................................................... 122
  Command Line Interface Syntax .................................................................................................... 122
    Connect ........................................................................................................................................ 122
    New ........................................................................................................................................... 123
Initialize ........................................................................................................................... 123
Update ................................................................................................................................... 124
Enroll .................................................................................................................................. 125
Moveuser ............................................................................................................................ 125
List ........................................................................................................................................ 126
Cd ......................................................................................................................................... 126
Delete .................................................................................................................................. 126
Help .................................................................................................................................... 127
Quit ..................................................................................................................................... 127

Revoking Tokens ............................................................................................................ 128
Revoke using the console ............................................................................................... 128
Revoke Options .................................................................................................................. 128
Rule-based Revocation ...................................................................................................... 130
Command Line Revocation ............................................................................................ 130

CHAPTER 9 – ADVANCED AUTHENTICATION ................................................................. 131

PreAuthentication Rules ................................................................................................. 131
Authentication Attributes ............................................................................................... 132
Agent is .............................................................................................................................. 132
Date Restrictions .............................................................................................................. 133
IP ......................................................................................................................................... 133
IP V6 .................................................................................................................................. 134
LDAP Password Pass Through ....................................................................................... 134
User is a member of ........................................................................................................... 135
User is in container ........................................................................................................... 135

Configuring Pre-Authentication Rules ........................................................................... 136
Authentication Activity Pane .......................................................................................... 137

CHAPTER 10 – INTERNAL SQL USER SOURCE CONTAINERS .................................... 138

Containers Tab .................................................................................................................. 138
Containers Group .............................................................................................................. 139
Users Group ...................................................................................................................... 140
CHAPTER 11 - HELP DESK

Secured Uses Tab

Secured User Search Group
User Search
Token Search
Secured Users Group
User Detail Group
Token Information Group
Access Restrictions Group
Authentication Metrics Group
Authentication Activity Group
Token Management Group
Details Button
Suspend Button
Unlock Button
Revoke Button
New PIN Button
Resync Button
Issue Button

Snapshot Tab

Authentication Activity Group
Systems Metrics Group
Authentication Metrics
Token Status
License Status
License Types

CHAPTER 12 – OPERATORS, ROLES AND REMOTE MANAGEMENT

Operator Tab
Operator Create
Roles
Help Desk
CHAPTER 13 - REPORTS ............................................................................................................... 163

Reports Tab ................................................................................................................................ 163

On-line Reports ................................................................................................................................ 163

System Summary Totals ............................................................................................................. 164

Token Summary Totals ............................................................................................................... 164

General Report Settings .......................................................................................................... 164

License Group ........................................................................................................................... 167

CHAPTER 14 - HIGH AVAILABILITY SOLUTIONS ........................................................................... 168

Single Location / Multi-site ........................................................................................................ 168

Multi-location / Multi-site ......................................................................................................... 169

Multi-location / Multi-site / Multi-master ................................................................................ 170

Multi-location / Multi-site / Cluster ......................................................................................... 171

Distributed Processing ............................................................................................................... 171

Virtualization .............................................................................................................................. 172

Configure Sites and Replication ............................................................................................... 173

Site Key and Configuration File ................................................................................................ 173

Site Export .................................................................................................................................. 173

Install additional site(s) ............................................................................................................. 174

CHAPTER 15 – SYSTEM BACKUP AND RESTORE ........................................................................ 176

PostgreSQL Database Backup and Restore ............................................................................... 178

Creating a backup of the BlackShield ID Database ................................................................... 178
Preface

BlackShield ID Documentation

For more information about BlackShield ID Authentication Platform, see the following documentation:

- Release Notes. Provides information about what is new and changed in this release, as well as workarounds for known issues.
- Getting Started. Lists what the kit includes (all media, diskettes, licenses, and documentation), specifies the location of documentation on the DVD or download kit, and lists CRYPTOCard Customer Support web sites.
- Administrator’s Guide. Provides information about how to administer users, tokens and security policy in BlackShield ID Authentication Platform.
- Migration Guide. Provides information for users moving from CRYPTOAdmin 5.x and CRYPTO-Server 6.x to BlackShield ID Authentication Platform 2.7, including changes to terminology and architecture, planning information, and installation procedures.
- Developer’s Guide. Provides information about developing custom programs using the BlackShield ID Authentication application programming interfaces (APIs).
- Performance and Scalability Guide. Provides information to help you tune your deployment for optimal performance.

Related Documentation

Additional documentation including interoperability and 3rd party integration guides are available at www.cryptocard.com.

Before You Call Customer Support

Make sure you have access to the server running the BlackShield ID Authentication Platform software.

Please have the following information available when you call:

- Your BlackShield ID License number. You can find this number in your license distribution media or in the BlackShield ID Manager by clicking the Details button in the Licenses Group on the System Admin tab.
- The BlackShield ID Authentication Platform configuration and software versions. You can find this by clicking the Details button in the Actions Group on the System Admin tab.
• The names and versions of the third-party products and applications that are authenticating against BlackShield ID.

• Details of the operating system version and service pack level on which BlackShield ID Authentication Platform or any Agents are installed.
Chapter 1 – About this Guide

This guide contains information about CRYPTOCard’s BlackShield ID v2.7 Authentication Manager Software package, including its installation and use.

Included in this manual are instructions on how to issue hardware, software, SMS zero-footprint and hybrid tokens. Detailed information about token types, installation on 3rd party platforms such as PCs, BlackBerry®, IronKey, Java phones and iPhone can be found in the respective token management and usage guides available at www.cryptocard.com.

New in BlackShield ID v2.7

In this software release, CRYPTOCard introduces:

- MP Token support for iPad 3.2 and iPhone iOS 4.0.2.
- Challenge-response support for user who have been assigned multiple tokens.
- SMS Quicklog tokens now support challenge-response.
- Self Service Site now supports the generation of GrIDsure grids.
- Added CellTrust to the list of available SMS Gateway Providers.
- BlackShield Authentication API now supports GrIDsure authentication.
- BlackShield Cisco AnyConnect Plug-in to allow the detection of MP tokens.
- BlackShield ID Agent for Remote Web Workplace under IIS 7.
- BlackShield ID Agent for Terminal Services Web and Remote Desktop Web under IIS 7.
- GrIDsure support for Cisco Clientless SSL VPN Access login.
- GrIDsure support for Juniper SSL VPN login.
Chapter 2 – Introducing BlackShield ID

BlackShield ID is an authentication platform that simplifies the implementation, management, control and provisioning tasks related to protecting a network from unauthorized access due to compromised logon credentials. In conjunction with CRYPTOCard hardware, software and zero-footprint tokens, BlackShield ID provides a formidable yet economical and easy to use solution to the problems and risks of shared, recycled and compromised passwords throughout the enterprise.

BlackShield ID Architecture

BlackShield ID is a web-services application that leverages Microsoft® Server technology and .NET to deliver a very high performance, scalable authentication service. The core application which provides all user, token and authentication services installs in IIS. Agents provide secure, redundant and encrypted communication links between BlackShield ID and protected access points, RADIUS servers and applications. Additional modules included with every licensed server provide automated token provisioning, self-service portals, secure self-enrollment and remote monitoring.

![Figure 1 - BlackShield ID Architecture]

**User Sources**

BlackShield ID can simultaneously provide authentication services for LDAP user sources as well as users created and managed within the internal SQL database. As a result, BlackShield ID can be used to extend authentication beyond corporate borders to include business partners, contractors and other external users.
BlackShield ID does not write to LDAP or modify the schema in any way. Changes in LDAP are immediately reflected and honored (Advanced Authentication, page 7) in BlackShield ID.

Multiple LDAP User Sources

Provided all UserID’s are unique, a single BlackShield ID instance can be configured to support multiple domains/LDAPs. For increased security, BlackShield ID connections to LDAP can be encrypted using SSL. Refer to LDAP External User Sources on page 21.

RADIUS

Referencing Figure 1, the IAS or NPS RADIUS Server components included with Microsoft Servers pass authentication requests from VPNs, firewall and other RADIUS clients to BlackShield ID via the IAS/NPS Agent. RADIUS support is essentially ubiquitous in networking hardware. As a result BlackShield ID can very often provide enterprise-wide authentication services for all network access points by simply enabling RADIUS wherever strong authentication is required.

BlackShield ID includes authentication agents for other RADIUS servers such as Funk / Juniper Steel Belted RADIUS.

Agents

There are several popular applications that do not have native RADIUS capability. Examples would include web-based applications such as OWA, SharePoint and Remote Web Workplace and versions of Citrix Web Interface prior to version 5.0. Installation of the appropriate Agents enables these applications to authenticate to BlackShield ID.
Authentication API

BlackShield ID includes an authentication API. This allows application developers to quickly build their own authentication agent using any programming language that supports SOAP and XML and is able to consume a web service. The typical development time for an agent is under 2 hours. For further information on the Authentication API refer to the document “BlackShield ID Authentication API”.

Basic Authentication

In simplest terms, BlackShield ID authenticates users at protected access points and applications by comparing the submitted logon credentials against the expected credentials. In a one-time password (OTP) context the easiest way to visualize the process is to view BlackShield ID as a duplicate of the users token for the duration of the logon. As a duplicate, the OTP generated by BlackShield ID should always match the OTP submitted by the authenticating user. And just like a token, the server generates and expects a different OTP for each logon.

BlackShield ID does support alternatives to OTP authentication including traditional passwords stored in the BlackShield ID database or in LDAP, primarily to facilitate a timed and controlled migration of large traditional password user populations to OTP authentication.

How user PINs are validated is really a question of security policy and token type. In Server-side PIN validation the user must prepend their PIN to the passcode, allowing BlackShield ID to receive and validate both components of the OTP. For example, if the PIN is ABCD, the user will submit ABCD + tokencode. Server-Side PIN can be used with all token types.
In Token-side PIN validation, the token will not generate a passcode until the user enters a valid PIN into the token. In this case only the tokencode is submitted to BlackShield ID for validation. Token-side PIN validation is typically used with MP software tokens and the RB-1 PIN Pad token.

In both cases the Security Administrator can establish PIN policies that determine the minimum length and strength of the PIN as well as the maximum number of consecutive incorrect PINs that may be submitted before an alert or Administrator intervention is required, thus protecting the user and the network against misuse of the token. In the event that a user forgets their PIN, the Security Administrator in the case of Server-side PINs can reset the PIN to a new value. In the case of a Token-side PIN¹, the Security Administrator can generate an “unlock” code that allows the user to create a new, policy compliant PIN for their token and generate passcodes.

The advantage of Token-side PIN policy is that PINs are never transmitted across the network, thereby mitigating the potential for exposure or capture. The advantage of Server-side PIN validation is that PIN policy can be modified at any time, allowing the Security Administrator to enforce periodic changes to strength, length and PIN change frequency.

The Self-service facility of BlackShield ID enables users to reset PINs without contacting the help desk.

**Advanced Authentication**

For complex networks, BlackShield ID Advanced Authentication can be used to simplify implementation, management and workflow by capitalizing on attributes associated with the users’ LDAP account such as group membership, access rights and account status.

¹ The ability to generate a Token-side PIN unlock code is a feature introduced with BlackShield ID v.2.5. This functionality is available for all RB tokens beginning with serial number 2023 or higher and all MP tokens, provided the tokens have been initialized with this feature enabled.
The following provides an overview of advanced authentication as shown in Figure 3 – Advanced Authentication.

**Source Agent and IP**

1. BlackShield ID validates the source of any incoming authentication request, allowing only a valid request to be processed. All other requests are immediately terminated. All security sensitive data is encrypted. PreAuth rules can allow some users to authenticate while denying others based on attributes such as the source IP of the authentication request (i.e. VPN).
Multiple User Data Sources

2. BlackShield ID searches for the UserID in the internal SQL database and LDAP. If the UserID is valid, the UserID\(^2\), including attributes such as account status, access restrictions and group membership are retrieved. If the UserID is invalid, the authentication attempt is rejected.

PreAuthentication Rules

3. PreAuthentication is arguably the most powerful function of BlackShield ID. It allows Security Administrators to create rules by which User attributes are evaluated and only if the evaluation is True is authentication allowed to proceed. For example; a simple rule could require the LDAP account be active and the group membership include “remote access”. In this way, only active LDAP accounts with remote access membership would be allowed to authenticate.

Since PreAuthentication rules can be applied to external user data sources, organizations can retain their existing user management workflow; Suspension or group membership changes performed in LDAP are automatically and immediately honored in BlackShield ID, solving one of the most common causes of compliance audit failure.

The above example is purposely simple. Far more sophisticated control and automation can be achieved using PreAuth. For a complete list of PreAuth functions and usage examples refer to Chapter 9 – Advanced Authentication on page 131.

\(^2\) In Active Directory the UserID may be modified or moved, therefore it is not a reliable identifier by which BlackShield ID can reference tokens associated with a user in the internal database. In Active Directory Domain Services, an accounts “objectGUID” property never changes, even if the object is renamed or moved, therefore BlackShield ID uses this property instead of the UserID. By using the objectGUID, BlackShield ID remains synchronized with Active Directory regardless of any modifications or movement of a user account in Active Directory.

For other LDAP servers BlackShield ID requires the equivalent of a GUID with a maximum length of 16 bytes to ensure consistent, synchronized association of tokens with LDAP user accounts.
Security Policy

4. The final step is validation of the OTP and where appropriate, application of Server-side PIN policy, including PIN changes and automatic resynchronization. A successful validation results in the user being granted access. A failed authenticate can generate help-desk alerts or activate protection against DOS and brute force attacks.

Note that other authentication methods and sequences are possible with BlackShield ID. For example, it is possible to require a user to successfully authenticate against LDAP using their traditional password before authenticating using an OTP. If using SMS zero-footprint tokens, a successful LDAP authentication could be used to trigger the delivery of the SMS/OTP.

Provisioning

Provisioning encompasses the steps that are required to:

- Enable Security Administrators to automate the assignment of tokens to 1 or more users in a single action.
- Provide for secure electronic or physical delivery of tokens to intended users.
- Support controlled, staged and transparent migration of users to tokens without interruption of service.
- Manage by exception whereby BlackShield ID generates alerts should any user fail to enroll within the terms of the security policy.
- Audit and report on all activity related to provisioning and enrollment.

The BlackShield ID management UI provides point and click provisioning, whereby tokens are assigned to users who are automatically emailed self-enrollment instructions. With the exception of hardware tokens which require physical delivery to the user, the Security Administrator is not required for any other part of the process.

Automated Bulk Provisioning

Automated bulk provisioning allows very large deployments to be accomplished with little effort. BlackShield ID offers two options for bulk provisioning:

- A Command Line Interface (CLI) that can bulk provision against a list of UserIDs. The CLI can be used by Security Administrators or by 3rd party provisioning software that support scripting such as Sun® Identity Manager.
- Rule-based provisioning whereby changes made in LDAP to user attributes such as becoming a member of a specified LDAP group can trigger the provisioning process without any intervention by the Security Administrator. Refer to Rule-based Provisioning on page 120.
Regardless of the provisioning method, choice of physical or electronic delivery method or PIN policy, token delivery is secure, as only the intended user is able to enroll and activate their token. In combination with PreAuth rules, Security Administrators can allow users continued use of their current authentication method until the token is enrolled, while at the same time establishing a timeframe by which enrollment must be completed. The “management by exception” function of BlackShield ID ensures that the Security Administrator is notified when enrollment exceptions occur, such as failing to enroll within the specified timeframe.

Self-enrollment

Self-enrollment is the process by which users securely enroll a token and seamlessly migrate to BlackShield ID authentication. As part of the provisioning process, users receive an email that includes instructions and a URL valid one-time only for enrollment. The instructions included with the email can be modified for content and branding. Refer to Chapter 18 - Customizing BlackShield ID on page 183.

The combination of provisioning and self-enrollment not only reduces the time commitment to issue tokens. It also eliminates any requirement for out-of-band communication with the end user, and the need to print, seal and send PINs.

For more information on Self-enrollment refer to Self-Enroll Function on page 116.

Customization and Internationalization

One of the most important aspects of security management is optimizing the experience for Security Administrators and for end users. With BlackShield ID you can:

- Modify the content, messaging and graphics presented to end users for services such as self-enrollment, self-service and email enrollment notifications. All text used by the system is contained in files that can be edited using a text editor such as notepad. This can include changes to language and instructions.
- All error messages produced by the system can be customized for language by editing text files.
- The UI can be modified by editing text files.
- The logo and backgrounds used on web pages can be modified.

For more information on Customization and Internationalization refer to Chapter 18 - Customizing BlackShield ID on page 183.
Chapter 3 – Tokens

In this chapter:

- Two-factor authentication
- Encryption standards
- Hardware tokens
- Software tokens
- Hybrid tokens
- SMS Zero-footprint tokens
- Battery replacement
- Privacy, Data Protection and Token Initialization
- Factory programmed tokens
- Unprogrammed tokens

CRYPTOCARD Tokens and Two-factor Authentication

To logon to network resources protected by BlackShield ID a user must enter a valid passcode. A passcode is a combination\(^3\) of:

- A personal identification number, or PIN (something the user knows)
- The tokencode currently displayed on the user’s token (something the user has)

Passcodes can be used almost anywhere a traditional password is used, often as a direct replacement or as an additional authentication layer. By requiring two factors, the BlackShield ID solution offers stronger security than traditional passwords (single-factor authentication).

For users familiar with the typical banking machine logon experience of card + PIN, the adoption of token + PIN as an alternative to traditional passwords will seem second-nature. When properly introduced, tokens are preferred by users because they reduce or eliminate the need to remember or periodically change

\(^3\) Generally accepted best practices require the use of a PIN, primarily to protect the token against unauthorized use. PIN policy including no requirement for a PIN is a matter of corporate security policy that in turn can be implemented in BlackShield ID. Regardless, a strong tokencode comprised of alphanumeric characters is superior to standard passwords due to the limitation of one-time use.
passwords. The token does this for them automatically, for each and every logon, effectively removing them from the password management equation.

The BlackShield ID Server supports the following token algorithms:

- AES (256-bit algorithm) tokens provide event or challenge/response authentication using the Advanced Encryption Standard (AES) cryptographic algorithm. AES seed records for factory programmed files are delivered in signed, encrypted file format (.btk). Records for unprogrammed tokens are generated by the BlackShield ID server.
- 3DES is the algorithm used with certain 3rd party event or challenge/response tokens that do not use a cryptographic processor that supports AES.
- OATH is the algorithm used with the UB-3 Oath compliant token.

**Token Selection**

The question of which token or combination of tokens to issue to users is answered by finding the optimum balance of convenience, cost and mobility that satisfies the organization’s security policy.

- Hardware tokens are tamper-resistant and tamper-evident devices and are machine independent, allowing a user to logon from any location or machine. For very large deployments, the auto-provisioning and self-enrollment features of BlackShield ID can substantially reduce the time and effort required to distribute hardware tokens to users.
- Software tokens are implementations of the hardware token that can be installed on a range of devices including hard drives, mobile devices such as BlackBerry®, Java phones, iPhones and secure flash drives such as IronKey® or SafeStick®, turning a device already in the hands of a user into a token. The advantage of software tokens is mass deployment without hardware distribution. By thoughtful selection of the type of device upon which a software

\[\text{AES (256-bit algorithm)} \]

\[\text{3DES} \]

\[\text{OATH} \]

---

4 The DES algorithm continues to be supported exclusively to accommodate legacy tokens imported from older servers. BlackShield ID will not allow DES for any other purpose. CRYPTOCard tokens shipped after January 1, 2004 use the AES 256-bit algorithm. All customers with tokens shipped between 1989 and 2004 are urged to trade-up to current hardware.
token can be installed, Security Administrators can lock a user to a specific machine, limit the user to using only secure platforms or provide complete machine independence. With BlackShield ID, software tokens can be issued, revoked and reissued without restriction or the need to recover the token from the user. With the exception of BlackBerry and Java phones, multiple MP software tokens can be installed on a single device (e.g. hard drive) provided the usernames are unique.

- Zero-footprint tokens, such as SMS, instantly turn any device capable of receiving an SMS message into a token without additional software or hardware. GrIDsure tokens also require no software installed on a users system other than the web browser included with Microsoft Windows.

- Hybrid tokens are hardware devices that offer a combination of complementary technologies such as photo identification and PKI functionality. As with hardware tokens, the auto-provisioning and self-enrollment features of BlackShield ID can substantially reduce the time and effort required to put tokens into the hands of users.
For more information on available token types, usage and options visit http://www.cryptocard.com.

Battery Replacement

Typically, CRYPTOCard tokens will operate for approximately 5-6 years before battery replacement is required. Depending on the model, the token display indicates a low battery condition about 2 months before failing.

Every CRYPTOCard RB-1 token holds 2 coin-cell batteries (CR-2016) and KT-4 hardware token holds 1 coin-cell battery (CR-2032). Battery replacement will permit the token to continue functioning.

Privacy, Data Protection and Token Initialization

Privacy and data protection legislation affects virtually all organizations connected to the internet while requirements for compliance continue to evolve. What is clear is that today’s practices will not be suitable in tomorrow’s world. Just as traditional password management has evolved to require ever more complex passwords and more frequent password changes, we can expect that token codes will also have to evolve to include something more than digits.

For this reason CRYPTOCard tokens have extended the aging industry standard of 6-digit token codes to allow up to 8 characters comprised of any combination of digits, letters and symbols. Through BlackShield ID, Security Administrators can adjust the strength of the tokencode to conform to the organizations security policy, auditor recommendations and the latest legislation through Initialization. Refer to Initialize Tokens on page 101.

This has 3 significant advantages:

- Tokens that are capable of generating high strength passcodes inherently provide a higher level of security.
- Higher strength passcodes result in higher user acceptance, since the need to enforce complex PINs comprised of digits, upper/lower case letters and other symbols upon the user to compensate for relative weakness of digit-only passcodes is eliminated.
Substantially improved total cost of ownership through a one-time investment in BlackShield ID coupled with tokens that don’t expire and can be customized for stringent privacy and data protection requirements.

**Factory Pre-programmed Tokens**

Preprogrammed tokens have been factory initialized and are ready for deployment to users, containing all operating parameters and programming necessary for proper function. All CRYPTOCard token types are available in pre-initialized format.

**Unprogrammed Tokens**

Unprogrammed tokens have not been factory initialized and rely on BlackShield ID to generate and apply encryption keys and other operating parameters through a process called initialization. Though the initialization process adds approximately 7 – 10 seconds to the time it takes to provision a user with a token, it has several advantages:

- Through initialization Security Administrators can modify the password strength and other operating parameters of a token, including factory initialized tokens. For example, this process could be used to upgrade the passcode strength from 6 digits to 8 alphanumeric characters.
- Token keys are not held outside of the organization using BlackShield ID.
- Encryption keys and other operating parameters can be changed before a token is reissued.
Software Tokens

Software tokens are implementations of the hardware token in software that can be installed on a range of devices including hard drives, mobile devices such as BlackBerry®, Java phones, iPhone and secure flash drives such as IronKey® Enterprise or SafeStick®, turning a device already in the hands of a user into a token.

The advantage of software tokens is mass deployment without hardware distribution. By thoughtful selection of the type of device upon which a software token can be installed, Security Administrators can lock a user to a specific machine, limit the user to using only secure platforms or provide complete machine independence. With BlackShield ID, software tokens can be issued, revoked and reissued without restriction or need to recover the token from the user.

Components

Software tokens are comprised of two components:

- The application software: this is a generic component that is common to all users of software tokens. It provides the user interface (GUI) and integration points with VPN clients and many web-based applications such as Citrix Web Interface, OWA and SharePoint.
- Initialization file: this is an encrypted file that contains all of the operating parameters of the token and is unique for each user.
Chapter 4 – Getting Started

In this chapter:

- Installation Prerequisites
- Virtualization
- Databases
- LDAP / Active Directory
- Multiple LDAP sources
- Supported Browsers
- Ports
- Agents
- Installation types
- Preparing to install

Please review the following information and ensure that the server upon which BlackShield ID is to be installed meets the minimum system requirements. BlackShield ID has been tested on 32 and 64 bit versions of Windows Server 2003 Standard, SBS 2003 R2 and Windows Server 2008 Standard and Enterprise Editions, using PostgreSQL 8.3, MySQL 5.1, Oracle 10g, Oracle 11g, Microsoft SQL Server 2005 and 2008.

Supported Operating Systems

- Windows Server 2003 (32/64bit)
- Windows Server 2008 (32/64bit)
- Windows Small Business Server 2003 (32 bit)
- Windows Small Business Server 2008 (32/64bit)
Supported Databases

- PostgreSQL 8.3 (default)
- MySQL 5.x
- MS-SQL 2005
- MS-SQL 2008
- Oracle 10g
- Oracle 11g

Supported LDAP Servers

- Active Directory
- Novell eDirectory 8.x
- Sun One 6.x

Architecture

- x86 / 32 bit
- x64 / 64 bit

Supported Internet Protocols

- IP v4
- IP v6

Software Requirements

- Microsoft Internet Information Services (IIS) 6.0 or 7.x with ASP.Net 2.0 enabled
- IAS (Windows 2003) or NPS (Windows 2008) if RADIUS authentication is required.
- .Net 2.0 and MSXML 6.0 SP1

---

5 The default database shipped with BlackShield ID is PostgreSQL. PostgreSQL does not support multi-master or two-way replication. Any other supported database must be downloaded and / or purchased separately.
Hardware Requirements

- Processor
  Minimum: 1 GHz (x86 processor) or 1.4 GHz (x64 processor)
  Recommended: 2 GHz or faster
- Memory
  Minimum: 512 MB RAM
  Recommended: 2 GB RAM or greater
- Available Disk Space
  Minimum: 100 MB
  Recommended: 100 GB or greater with logging enabled
- Display
  SVGA (1024 x 768), 24-bit colour or higher

Other Requirements

- Installation requires that the Security Administrator installing BlackShield ID have administrative rights on the localhost.
- If upgrading or moving BlackShield ID to another server refer the Upgrading BlackShield ID Guide.

Virtualization

BlackShield ID is designed for virtualization and has been extensively tested with VMWare®.
Internal Database

The internal database contains all system configuration, application and policy data, token, history and activity information used by BlackShield ID. If configured as a User Source, it will also contain user specific information such as UserIDs and coordinates. Where LDAP/AD integration is configured, the unique “GUID” property of the user account is stored in the database, providing a consistent link between LDAP and BlackShield ID. The UserID is stored with authentication activity for reporting purposes. This allows BlackShield ID to provide audit trails and authentication activity reports even after a User (and therefore the GUID) has been deleted from LDAP.

The database can be installed on the machine hosting BlackShield ID, on a separate machine or as a cluster. Every BlackShield ID server can be configured for a primary database instance with failover to an alternate instance. In addition, multiple BlackShield ID servers can use the same database.

LDAP External User Sources

BlackShield ID supports the use of one or more LDAP directories for User, Account Status and Group Membership data.

---

6 Support for multiple concurrent LDAP user sources requires that UserIDs be unique across all LDAPs.
By default BlackShield ID connects to LDAP over ports 389 or 636 (LDAPs / SSL). While SSL is recommended, BlackShield ID does not send sensitive data to LDAP in the clear. The primary reason for SSL is to protect account information and group membership data transmitted to BlackShield ID.

BlackShield ID includes a default Active Directory, Novell eDirectory 8.x and Sun One 6.x object mapping template. Refer to System Settings: Users on page 54.

BlackShield ID does not write to or modify the LDAP schema.

**Supported Browsers**

The standard interface with BlackShield ID or components such as self-enrollment and user self-service is a browser. The following browsers are supported:

- Windows platforms
  - Internet Explorer 6
  - Internet Explorer 7
  - Internet Explorer 8
- Firefox 3+
- Linux
  - Firefox 3+

Certain functions may require ActiveX controls and/or JavaScript.
Ports

BlackShield ID may require the following ports, depending upon the location of external directories, databases or RADIUS servers. The following is a list of default port values. BlackShield ID can be configured to use alternate ports. SSL requires that a valid certificate be installed on the BlackShield ID server.

<table>
<thead>
<tr>
<th>Port (TCP/UDP)</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>80 / 443</td>
<td>Port 80 and/or 443 can be used for management sessions, provisioning, Self-enrollment, Self-service and to service encrypted authentication requests from configured Agents. For security purposes port 443 (SSL) is recommended.</td>
</tr>
<tr>
<td>1812/1813</td>
<td>Ports 1812/1813 are standard ports for RADIUS authentication and RADIUS accounting respectively.</td>
</tr>
<tr>
<td>389/636</td>
<td>Ports 389/636 are standard ports for LDAP and LDAPS connections respectively. For security purposes port 636 (SSL) is recommended.</td>
</tr>
<tr>
<td>5432</td>
<td>The port number for connection to the default PostgreSQL database.</td>
</tr>
<tr>
<td>1433</td>
<td>The default port number for connection to a MS-SQL database.</td>
</tr>
<tr>
<td>1521</td>
<td>Oracle</td>
</tr>
<tr>
<td>3306</td>
<td>MySQL</td>
</tr>
</tbody>
</table>

Agents

Agents are installed on resources that are to be protected by BlackShield ID that do not natively support RADIUS authentication. Agents receive authentication requests, reformat the requests into SOAP packets, encrypt all security sensitive data using AES 256 bit encryption, and then forward the requests to BlackShield ID. Agents are configurable for failover and will automatically recover when the primary authentication path is restored. In high availability scenarios, a load balancer may be placed between Agents and BlackShield ID servers.
Figure 7 – RADIUS Agents and Failover

Agents are included in the BlackShield ID distribution and may be downloaded from http://www.cryptocard.com.

Maintaining Accurate Time Settings

BlackShield ID operation and authentication services are not dependant on accurate time settings. However best practices recommend that accurate time be maintained to achieve reliable and consistent reporting and audit trails. In some cases BlackShield ID licensing may restrict certain functions based on dates or date ranges. Modifying the server date after license installation may cause these functions to become unavailable.

CRYPTOCard recommends that the BlackShield ID server time be set to the local zone and that the server time be UTC coordinated. For more information go to http://www.time.gov.

Installation Types

A BlackShield ID site is defined as an instance of the BlackShield ID authentication engine. The number of sites and configuration options are determined by licensing, redundancy and performance requirements. Assuming BlackShield ID is installed on recommended hardware, the factor that has the largest bearing on performance is database I/O, primarily determined by the amount and frequency with which authentication history is written. In most cases it is acceptable to have the database and BlackShield ID installed on the same server.

The following scenarios are provided as guidelines and examples. Many different configurations are possible. For example, it is perfectly acceptable to install the database, enrollment, self-service and directory components on separate machines. Contact CRYPTOCard or your local supplier for recommendations on a configuration that would best meet your performance, availability and maintenance requirements.
Small Business Server Deployments

BlackShield ID server and components including the database, agents for RADIUS, IIS, OWA, RWW and SharePoint can be installed on Microsoft 2003 or 2008 Small Business Server. This solution is ideal for organizations using Small Business Server and authentication support for up to 75 users.

![Small Business Server Deployments Diagram](image)

**Figure 8 – Small Business Server Deployments**

Small, Single-Site Deployments

Single-site deployments supporting up to 2500 users may choose to install all BlackShield ID components on a single server with a secondary instance providing redundancy and failover.

![Small Deployments with Failover Diagram](image)

**Figure 9 – Small Deployments with Failover**

Authentication and management functions can be distributed across the sites if necessary. Agents can failover to the alternate site.
The connections between LDAP and BlackShield ID can be local or remote. In the event that there is a primary and secondary LDAP server, each BlackShield ID instance would normally be configured for LDAP failover.

Enrollment and Self-service modules can be installed on the BlackShield ID server or on a remote server.

Medium Site Deployments

The medium site deployments are typically required for organizations that have dedicated LDAP, Web and RADIUS servers. In this scenario, the database replication is handled between BlackShield ID instances.
Figure 11 – Medium Deployments

Large Deployments

For sites requiring support for up to 250,000 users and several hundred authentications/second, use of a database cluster fronted by multiple BlackShield ID servers is recommended.

Figure 12 – Large Deployments

What you need to begin

- CRYPTOCard recommends downloading the most recent version of BlackShield ID from http://www.cryptocard.com
- If this is a new installation you will need a valid BlackShield ID license (.blc extension) and activation key. These are emailed to you by CRYPTOCard. Contact your supplier if you have not received a license.
- If this is an upgrade from CRYPTOAdmin 5.x or CRYPTO-Server 6.x server product refer to Appendix A – Upgrading from CRYPTOAdmin 5.32 on page 187 or Appendix B – Upgrading from CRYPTO-Server 6.x on page 190 respectively.
- If Active Directory will be a User data source for BlackShield ID it is recommended that you create an account in Active Directory that can be used by BlackShield ID to connect to the directory. The only requirement is that the account have sufficient privileges to browse the directory OUs containing users. We recommend that an account name such as “blackshield”
that reflects the application be used so that it can be distinguished from other user accounts.

NOTE: The account password used by BlackShield ID to connect to LDAP must be set to “never expire”

**Standard Installation**

The standard installation option installs BlackShield ID with the default database on the primary drive. All configuration is post installation.

**Custom Installation**

Custom installation provides the option to bypass installation of the default database. Choose this option if you already have an existing compatible database that you wish BlackShield ID to use, you wish to install BlackShield ID to a different drive location or you wish to install the Salesforce.com delegated authentication module. Compatible databases are:

- MySQL 5.0+
- Oracle 10g/11g
- MS-SQL 2005/2008
- MS-SQL Express

---

While MS-SQL Express is a supported database, those choosing to use it should be aware of its limitations with respect to database size, backup and replication. Use of this database is recommended only for small deployments and only if local technical support is available to manage regular backups. CRYPTOCard does not provide technical support for optional databases.
Chapter 5 – Installing BlackShield ID Server and RADIUS

In this chapter:

- Installing BlackShield ID
- Configuring Microsoft IAS RADIUS
- Configuring Microsoft NPS RADIUS Component
- Installing BlackShield ID Agent for IAS
- Installing BlackShield ID Agent for NPS
- Configuring the BlackShield ID Agent for NPS/IAS

Installation BlackShield ID Server

The installation process takes approximately 10 minutes. On completion the BlackShield ID Authentication, Console, Enrollment and Self-service application pools will have been created in IIS. A BlackShield ID Self-service web site will have been created and the BlackShield ID auto-provisioning and Monitor services will be started. Finally, a CRYPTOCard/BlackShield ID/ program group will have been created under the Start Menu.

On-line configuration instructions are available through the CRYPTOCard/BlackShield ID/ program group.

To install BlackShield ID:

1. Log on to the server on which BlackShield ID will be installed using a localhost administrator credential or a domain administrator credential with localhost administrator rights.

2. Locate and run the BlackShield ID Installer:
   - BlackShield IDProfessional.exe for 32 bit servers
   - BlackShield ID Professional x64.exe for 64 bit servers.

3. Accept the license agreement to continue with the installation.

4. Select “Complete” to install all components including the default database to the primary drive.
   Select “Custom” if any of the following apply:
   - You already have an existing compatible database that you wish BlackShield ID to use.
   - You wish to install BlackShield ID to a different drive location.
   - You wish to install the Salesforce.com delegated authentication module. (Refer to Custom Installation on page 28 for a list of supported databases).
Installing RADIUS

BlackShield ID uses the IAS or NPS RADIUS components of Windows Server 2003 or 2008 respectively. To enable BlackShield ID to accept RADIUS authentication requests you must:

- Install either the Windows IAS or NPS Windows component.
- Install the BlackShield ID Agent on the machine hosting IAS or NPS.

![Figure 13 - RADIUS Servers and Agents](image)

RADIUS requests received by IAS/NPS from devices such as VPNs, firewall and other RADIUS “Clients” are passed to BlackShield ID via the installed Agent.

![Figure 14 – RADIUS Server Locations](image)

IAS/NPS can be installed on the BlackShield ID server or on a separate server. The Agent can be configured to failover to a backup BlackShield ID server in the event that the primary cannot be contacted. It will automatically reconnect to the primary when it becomes available.
Note that the IAS/NPS components must be configured to accept RADIUS authentication requests from RADIUS Clients. At a minimum this means that IAS/NPS must be configured for the IP address, shared secret and port number for each RADIUS Client. A corresponding configuration must be made at the RADIUS Client.

RADIUS Client configuration guides for a wide range of VPN, firewall and other network access devices are available in the solutions section of http://www.cryptocard.com/.

It is good practice to test an “end-to-end” RADIUS authentication using static passwords before installing the Agent. This simple step eliminates the possibility of RADIUS configuration errors, which will result in the Agent not receiving data from IAS/NPS.

**Preparation and Prerequisites**

1. Verify that a “Test” user account can successfully authenticate against IAS/NPS using a static password prior to installing the Agent.

2. The Agent communicates with BlackShield ID over either port 80 or 443 by default though other ports may be used. In any case, if IAS/NPS is installed on a separate server ensure that the chosen port is open on all firewalls between the Agent and the BlackShield ID server.

3. Assign a temporary password in BlackShield ID to the “Test” user account.

**Installation**

- Installation and configuration instructions for use with Microsoft IAS begin with Configure Microsoft IAS for RADIUS Client(s) on page 32.
- Installation and configuration instructions for use with Microsoft NPS begin with Configure Microsoft NPS for RADIUS Client(s) on page 38.

The instructions for configuring the Agent after installation are common to both IAS and NPS. Once installation is complete, refer to the section: Configure the BlackShield ID Agent for IAS / NPS on page 41.
Configure Microsoft IAS for RADIUS Client(s)

1. Open the “Internet Authentication Service Console”
2. Select “RADIUS Clients”
3. Right click client and select “New RADIUS Client”
4. Enter “Friendly name” of your remote client (i.e. SSL VPN Authentication)
5. Enter the “IP address” of the client (i.e. VPN Device)
6. Click “Next”
7. Select Client-Vendor of “RADIUS Standard”
8. Enter “Shared secret”. This must match the shared secret on the client end.
9. Enter “Confirm shared secret”
10. Click “Finish” to add client

IMPORTANT: These changes will not take effect until the IAS service has been restarted. Do this from the Windows Service manager or from a DOS command prompt as follows:

C:\> Net stop IAS
C:\> Net start IAS
Installation BlackShield ID Agent for IAS

Locate and run the Agent installer:

- BlackShield ID NPS IAS Agent.exe for 32 bit servers
- BlackShield ID NPS IAS Agentx64.exe for 64 bit servers

1. Log on to the server on which IAS or NPS has been installed.

2. Locate and run the BlackShield ID Installer:
   BlackShield ID NPS IAS Agent.exe for 32 bit servers
   BlackShield ID NPS IAS Agent x64.exe for 64 bit servers.

3. Accept the license agreement to continue with the installation.

4. Enter the hostname or IP address of the primary BlackShield ID Server.
   To use SSL install a valid certificate on the IAS / NPS server.
   Tick the check box and add the hostname or IP address of a failover BlackShield ID server if available.
   Click Next.
Configure IAS to use BlackShield ID Agent

On completion the installer will offer to display the agent configuration documentation. This documentation as well as an agent configuration management tool is available through the Start Programs / CRYPTOCard / BlackShield ID NPS/IAS Agent program group.

Create a Remote Access Policy

1. Open the “Internet Authentication Service Console”
2. Select the “Remote Access Policies”
3. Select the first policy in the right hand pane, if one exists.
4. Select “Remote Access Policies” again
5. Right click and select “New Remote Access Policy”

A Wizard should pop up. Click “Next” to dismiss welcome dialogue.

6. Select “Set up a custom policy”
7. Enter a friendly policy name of “Authenticate to BlackShield”
8. Click Next.
9. Click Add

10. Select “NAS-Port-Type”

11. Click Add

12. Select “Ethernet”, then click Add

13. Select “Grant remote access permission”

14. Click Next

15. Click Next to skip changing the profile

16. Click Finish to add the policy.
Create a Connection Request Policy

1. Open the “Internet Authentication Service Console”
2. Expand Connection Request Processing
3. Select Connection Request Policies
4. Select the first policy in the right hand pane, if one exists.
5. Select Connection Request Policies again
6. Right click and select New Connection request policy
7. A Wizard should pop up. Click “Next”
8. Select A custom policy
9. Enter a policy name of “Allow all users to authenticate with BlackShield”
10. Click Next
11. Click Add
12. Select Day-And-Time-Restriction
13. Click Add
14. Click “Permitted”
15. Click OK and then click Next.
16. Click Edit Profile

17. Click Accept Users without validating credentials.

18. Click OK.

19. Click Next.

20. Click Finish to add the policy.
Configure Microsoft NPS for RADIUS Client(s)

1. Open the “Network Policy Server Console”
2. Select “RADIUS Clients”
3. Right click client and select “New RADIUS Client”
4. Ensure that the textbox for “Enable this RADIUS Client” is selected
5. Enter “Friendly name” of your remote client (i.e. SSL VPN Authentication)
6. Enter the “IP Address” of the remote client (e.g. VPN device)
7. Select “Vendor name” of “RADIUS Standard”
8. Select Client-Vendor of “RADIUS Standard”
9. Enter “Shared secret”. This must match the shared secret on the client.
10. Re-enter the shared secret in the “Confirm shared secret”
11. Click “OK” to add client

IMPORTANT: These changes will not take effect until the Network Policy Server has been restarted.
Installation BlackShield ID Agent for NPS

Locate and run the Agent installer:

- BlackShield ID NPS IAS Agent.exe for 32 bit servers.
- BlackShield ID NPS IAS Agentx64.exe for 64 bit servers.

1. Log on to the server on which IAS or NPS has been installed.
2. Locate and run the BlackShield ID Installer:
   - BlackShield ID NPS IAS Agent.exe for 32 bit servers
   - BlackShield ID NPS IAS Agent x64.exe for 64 bit servers.
3. Accept the license agreement to continue with the installation.
4. Enter the hostname or IP address of the primary BlackShield ID Server.
   - To use SSL install a valid certificate on the IAS / NPS server.
   - Tick the check box and add the hostname or IP address of a failover BlackShield ID server if available.
   - Click Next.
Configure NPS to use BlackShield ID Agent

On completion, the installer will offer to display the agent configuration documentation. This documentation as well as an agent configuration management tool is available through the Start Programs / CRYPTOCard / BlackShield ID NPS/IAS Agent program group.

Creating a Connection Request Policy

1. Open the “Network Policy Server Console”
2. Expand “Policies”
3. Select “Connection Request Policies”
4. Right Click and select “New”
5. The “New Connection Request Policy” Wizard begins
6. When prompted enter a policy name of “Allow all users to authenticate with BlackShield”
7. Under “Type of network access server” select “Remote Access Server (VPN-Dial up)”
8. Click “Next”
9. Click “Add” from the “Specify Condition” dialog
10. Select “Date and Time Restrictions”
11. Click “Add”
12. Select “Permitted” and click “OK”

13. Click “Next”

14. In the next dialog select “Accept users without validating credentials”

   NOTE: This causes authentication requests to be intercepted by the BlackShield ID agent. This setting is required in order to allow the agent to function correctly.

15. Select “Next”

16. Select “Next”

17. Click “Finish” to add the policy

18. Under “Connection Request Policies”, right click on “Use Windows Authentication for all users” and select “Disable”

---

**Configure the BlackShield ID Agent for IAS / NPS**

To launch the BlackShield ID Configuration Tool, click Start > All Programs > CRYPTOCard > BlackShield ID NPS IAS Agent > Configuration Tool.
NPS/IAS Settings

Agent Activation
Turns the BlackShield ID Agent on or off.

IP Address Detection
Provides the ability to detect and send the remote client IP address to BlackShield

Migration Mode
Allows users to proxy the authentication request to the next server listed in the Remote RADIUS Server Groups within NPS or IAS.

NPS/IAS Trace
Turn on verbose logging within NPS or IAS

Communication Settings

Authentication Server Settings
Used to configure the IP address / hostname of the primary and failover BlackShield ID Servers. Default is port 80, alternate is 443 (SSL).

Timeout Settings
Sets the maximum timeout value for authentication requests.

Encryption Settings
Used to browse to the BlackShield ID Agent Key File.
Authentication Test

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

Logging Level

Adjust the logging level. Default is set to Log Level 3, which will only log information from Warning to Critical.

Log File Location

Browses to the log file location. The default location is:

\Program Files\CRYPTOCARD\BlackShield ID\IAS Agent\Logs

For log levels, 1, 2 and 3, only the initial connection between the Agent and the Server and any failed connection attempts are logged.

Note that the IAS/NPS service must be restarted for changes to log settings to take effect.
Localization

Edit Resource Strings

The settings in this tab represent the prompts and information messages provided to the RADIUS client (and user). These can be modified in this section as necessary to improve usability.

Note that the default location of the resource string file is the \languages\en folder. Since upgrade of the agent will overwrite any changes made in this directory. To avoid losing changes, refer to Chapter 18 - Customizing BlackShield ID on page 183.
Chapter 6 – Configuring BlackShield ID

In this chapter:

- Basic configuration
- Advanced configuration

Basic BlackShield ID Configuration

This section deals only with mandatory configuration items. Advanced and optional configuration is detailed in Advanced Configuration - System Admin Tab on page 64.

All configuration of BlackShield ID is done post installation. It is a highly configurable application however only a few configuration items are mandatory. The final step of installation will offer to launch the BlackShield ID Manager. At any time it can be launched from the Start Menu group.

Initially remote management is disabled and only an administrator account on the localhost or a domain admin account is valid for logon to the manager. You will have the opportunity to allow remote management and alter the logon requirements after initial configuration is complete.

At the logon prompt enter your localhost administrator credentials.

You will automatically be redirected to the System Admin tab where all system configuration options can be configured. Figure 16 on page 46 shows all configuration items available on this tab once basic configuration is complete.

Initially basic configuration items are displayed in the order in which they must be completed:

- System Settings: SQL
- Licenses:
- System Settings: Users
Actions Group

The buttons in this group are used in conjunction with changes made on the System Admin tab. Depending on the configuration status of the server, buttons will be enabled or disabled.
Apply  This button will be enabled if required to save a configuration change.

Cancel  Cancels any unapplied changes.

Status  Tests various systems and reports their status.

Green: system is functioning properly.

Yellow: some services may not be available or degraded, depending upon the server configuration. For example, referencing Figure 17 - System Status.

Red: indicates that a required component is not available and will cause any service that relies on the component to fail. For example, if SMTP is red, the server will not be able to send alerts or enrollment messages by email.

Details  Generates a file that captures all configuration items from the System Admin and Policy Admin tabs. It also includes server version and sub component version information.

Sites  This function is used when creating replica/failover servers and is covered in Chapter 14 - High Availability Solutions starting on page 168.

**System Setting: SQL**

BlackShield ID stores all token related data and authentication history in a SQL database. If you chose to install the default database, all tables have been created and the connection status should indicate “Connection Active”.

An issue with the SSL certificate may inhibit or prevent the use of SSL connections between BlackShield ID and LDAP, remote management sessions and self-enrollment sites configured for https.

Red: indicates that a required component is not available and will cause any service that relies on the component to fail. For example, if SMTP is red, the server will not be able to send alerts or enrollment messages by email.

---

**Figure 17 - System Status**

![System Status Diagram]
To change the default database logon credentials used by BlackShield ID or configure a failover database refer to Chapter 14 - High Availability Solutions starting on page 168.

**Alternative Database Configuration**

Skip to the appropriate section indicated below if you opted not to install the default database in favor of one of the supported database alternatives:

- MySQL 5: refer to MySQL 5.x Database Configuration on page 49
- Microsoft SQL Server: refer to MS-SQL Database Configuration on page 51
- Oracle 10g / 11g: refer to Oracle Database Configuration on page 53
MySQL 5.x Database Configuration

BlackShield ID and a MySQL 5.x database.

1. Create a MySQL Server account and password that will be used by BlackShield ID to connect to the SQL server. This account must have full read/write/create/delete capability.

2. Click Configure

3. Select MySQL from the Connection Type dropdown

   Enter the following information:

   Server: this is the hostname or IP address of the MySQL server. NOTE: do not use localhost or loopback address if you intend to configure additional BlackShield ID sites or failover.

   Port: The default MySQL port is 3306. Do not change this value unless your MySQL instance is configured for a different port number.

   User Name: This is the account that BlackShield ID will use to connect to MySQL.

   Password: This is the password that BlackShield ID will use to connect to MySQL.

4. Do not enter anything in these fields during initial configuration of the primary server.

   These values are the hostname or IP address of failover MySQL databases. Note that the username and password used by BlackShield ID to connect to these databases must be the same as that used in step 3.

   These values should only be created by rerunning the configuration wizard after the primary MySQL database has been completed.
5. Click Next to create the database tables.

**IMPORTANT:** For highest security copy the cipher.bak and cipherkey.txt files created in the CipherExport Directory to a secure location. These files are necessary to restore the database or move the database to another server. Without these files it will not be possible for anybody to copy, move or restore the database. You may want to consider making an additional backup of this data in an alternate secure location.
MS-SQL Database Configuration

BlackShield ID can use Microsoft SQL Server 2005 or 2008 provided the database has been configured for Mixed Mode authentication. To change an existing installation to support Mixed Mode authentication refer to the Microsoft article: http://msdn2.microsoft.com/en-us/library/ms188670.aspx.

Create a SQL Server account and password that will be used by BlackShield ID to connect to SQL server. This account must have full read/write/create/delete capability.

1. Click Configure.

2. Select MS SQL from the Connection Type dropdown.

   Enter the following information:

   Host: This is the Server Name or IP address of the MS-SQL Server. NOTE: do not use localhost or loopback address if you intend to configure additional BlackShield ID sites or failover.

   Database: This is the name of the database to be created and used by BlackShield ID. Any valid database name is acceptable. The default is BlackShield.

   User Name: This is the SQL account name that will be used by BlackShield ID to log onto SQL Server.

   Password: This is the password that will be used by BlackShield ID to log onto SQL Server.

   During initial configuration do not tick the Failover Host tick box. Use this option only after the primary site has been created and a second MS-SQL server instance has been created. Rerun the wizard to update this field.

   Click Save to store the configuration.

3. Click Next to create the database tables.
4. Copy the cipher.bak and cipherkey.txt files created in the CipherExport Directory to a secure location. These files are necessary to restore the database or move the database to another server. Without these files it will not be possible for anybody to copy, move or restore the database.
Oracle Database Configuration

BlackShield ID can use Oracle 10g or 11g database. The connection is created via the Oracle Data Access Components (ODAC) client. The following must be configured prior to using BlackShield ID with an Oracle database:

1. The Oracle Data Access Components (ODAC) client 11g or higher must be installed. This is part of the Oracle client software; please refer to the Oracle website (http://www.oracle.com) for more information.

2. A Net Service Name must exist on the BlackShield ID server to connect to the Oracle database (in most cases, this is created using the Oracle Net Configuration Assistant).

3. An Oracle user account must exist to allow the BlackShield ID server to connect to the database.

4. Click Configure.

5. Select Oracle from the Connection Type dropdown.

   Enter the following information:

   Net Service Name: from step 2 above.

   User Name: from step 3 above.

   Password: from step 3 above.

6. Click Next to create the database tables.

7. Copy the cipher.bak and cipherkey.txt files created in the CipherExport Directory to a secure location. These files are necessary to restore the database or move the database to another server. Without these files it will not be possible for anybody to copy, move or restore the database.
Licenses

BlackShield ID requires that a valid license be installed on the system. The license consists of two parts: a license file which determines the capability of the server including the maximum number of tokens that may be issued, and a corresponding Activation Key.

Use the browse button to locate the license file which will have a .blc extension and be in the format of XX-yyyyyy.zzz.blc. Copy and paste the 26 character Activation key delivered with the license into Activation Key field, then click “Import”.

All subsequent licenses are installed using this procedure.

System Settings: Users

BlackShield ID can use LDAP, SQL or both as a user data source:

- If configured for LDAP, users from LDAP will automatically appear or be removed from BlackShield ID as they are being added or removed from LDAP.
- If configured for SQL, BlackShield will allow users to be created in the SQL database by using the BlackShield ID Manager or will allow users to be imported from a flat file using the command line utility (Command Line Interface (CLI) Provisioning on page 122).
- If configured for both LDAP and SQL, BlackShield ID will concurrently support both user sources. Organizations that have their internal users in LDAP but wish to extend authentication services to external user account not in LDAP (such as contractors or customers) should choose this option.

The choice of user data source can be modified at any time, provided that care is taken to ensure that there is no conflict caused by duplicate User IDs and that the relationship between tokens and users is not severed during reconfiguration. For assistance or guidance when reconfiguring contact your supplier or CRYPTOCard Customer Support.

The following steps describe configuration for both LDAP and SQL. A subset of these steps corresponds with the selection of LDAP only or SQL only user source.

1. Click the Configure button in the System Settings: Users group then click Next.

2. For first time configuration ensure the Setup a new connection radio button is selected, then click Next.
LDAP User Source Configuration

3. Select LDAP and SQL from the User Source dropdown then click Next.

4. Select 1 from the dropdown as the number of Domains for which BlackShield ID will provide authentication services then click Next.

5. Enter a descriptive name for the Domain in the Domain Name field then click Next. The name should be informative to BlackShield ID administrators. This name will appear in UI whenever users from this domain are being managed.

6. Enter the host name or IP address of the LDAP server. The default of localhost assumes BlackShield ID has been installed on the same machine hosting LDAP (such as Microsoft Small Business Server).

   Do not alter the default port number 389 unless your LDAP has been specifically configured to use a different port number.

   BlackShield ID can use SSL for connections to LDAP provided a valid certificate has been installed on the server.

   The Number of Failover hosts is used to configure alternate LDAPs should the primary LDAP configured above be unreachable by BlackShield ID. Selecting a number from the drop down list will allow the Domain Name or IP address of the corresponding alternate LDAPs to be configured.

7. BlackShield ID can be configured to use an Active Directory, Novell eDirectory or Sun One 6.x schema. Select the LDAP Schema type then click Next.
Custom Schema Support

If your directory uses a custom schema or you are using a different type of LDAP server it may be necessary to modify the BlackShield ID LDAP mappings. Click the Edit button to access the mappings table.

Edit the LDAP object references according to your schema.

BlackShield ID allows up to 3 LDAP objects to be mapped to custom fields displayed on the Secured Users and Assignment tabs. Enter the LDAP object references to be used to populate these fields in the UI.

To finish the mappings, modify the Schema Name, then click Apply. Be sure to select the new schema mapping in the Choose LDAP Schema dialogue before continuing.

8. Enter the LDAP account to be used by BlackShield ID to connect to and browse LDAP. If you are not familiar with User DN syntax you can use the account’s email address and password. If the LDAP directory supports an anonymous bind, leave the UserDN and Password field blank.

9. BlackShield ID automatically scans LDAP and retrieves a list of all containers with users and provides an option to add all containers to or exclude some containers from BlackShield ID.

To add all containers with users to BlackShield ID, click Next.

Users Found

BlackShield has scanned the LDAP server and optimized its search scope to include containers where users currently exist and their sub containers.

[Manual edit checkbox]

Note: Only containers that currently have users will be added.
To prevent a container with users from being available in BlackShield ID for viewing, token assignment or authentication, place a check in the “Manually edit searched Containers” checkbox, remove the corresponding DN entries, then click Next.

10. The Choose Provider dialogue is used to create the internal user data source to be used by BlackShield ID to create and manage user accounts that do not exist in LDAP. Normally this will be the same database configured under System Settings: SQL on page 46) though this option allows a different database to be selected for this purpose.

Note that BlackShield ID prevents creation of a UserID in the internal database that already exists in LDAP. In addition, if a UserID is created in the internal database and subsequently an identical UserID is created in LDAP, the following will occur:

- The UserID in the internal database will be removed
- Any tokens assigned to the removed UserID will be marked as "Lost" with a comment in the history record indicating a duplicate name was found in LDAP.

Internal SQL User Source Configuration

The following describes the steps to configure the default database to be a User data source.

Skip to the appropriate section indicated below if you opted not to install the default database in favor of one of the supported database alternatives:

- MySQL: refer to MySQL User Data Source on page 59
- Microsoft SQL Server: refer to MS-SQL User Data Source on page 61
- Oracle 10g/11g: Oracle User Data Source on page 63

To use the default database:

11. Select PostgreSQL from the dropdown
12. This dialogue will be complete except for the Password required to logon to the database. Use the same password provided in System Settings: SQL. The default PostgreSQL password can be found in the BlackShield ID Configuration link within the CRYPTOCard Program Group.

13. Click Next to create the necessary tables in the database.

14. Click Done to save configuration.

15. The System Setting: Users will now show a connection status of Active. At this point all of the optional configuration items available under the System Admin tab will be displayed.
MySQL User Data Source

This section applies only if using MySQL as a database.

11. Select MySQL from the dropdown

12. Enter the following information:
   
   Server: this is the hostname or IP address of the MySQL server. NOTE: do not use localhost or loopback address if you intend to configure additional BlackShield ID sites or failover.

   Port: The default MySQL port is 3306. Do not change this value unless your MySQL instance is configured for a different port number.

   User Name: This is the account that BlackShield ID will use to connect to MySQL.

   Password: This is the password that BlackShield ID will use to connect to MySQL.

13. Do not enter anything in these fields during initial configuration of the primary server.

   These values are the hostname or IP address of failover MySQL databases. Note that the username and password used by BlackShield ID to connect to these databases must be the same as that used in step 12.

   These values should only be created by rerunning the configuration wizard after the primary MySQL database has been completed.
14. Click Next to create the database tables.

15. Click Done to save configuration.

16. The System Setting: Users will now show a connection status of Active. At this point all of the optional configuration items available under the System Admin tab will be displayed.
MS-SQL User Data Source

This section applies only if using MS-SQL as the database.

11. Select MS SQL from the dropdown

12. Enter the following information:

   Server: this is the hostname or IP address of the MS-SQL server. NOTE: do not use localhost or loopback address if you intend to configure additional BlackShield ID sites or failover.

   Port: The default MS-SQL port is 1433. Do not change this value unless your MS-SQL instance is configured for a different port number.

   User Name: This is the account that BlackShield ID will use to connect to MS-SQL.

   Password: This is the password that BlackShield ID will use to connect to MS-SQL.

13. Do not enter anything in the Failover host field during initial configuration of the primary server.

   This value is the hostname or IP address of failover MS-SQL databases.

   These values should only be created by rerunning the configuration wizard after the primary MS-SQL database has been completed.

14. Click Next to create the database tables.
15. Click Done to save configuration.

16. The System Setting: Users will now show a connection status of Active. At this point all of the optional configuration items available under the System Admin tab will be displayed.
Oracle User Data Source

This section applies only if using Oracle as the database.

11. Select Oracle from the dropdown

12. Enter the following information. This should be the same as configured in step 2 and 3 of Oracle Database Configuration on page 53.

13. Click Next to create the database tables.

14. Click Done to save configuration.

15. The System Setting: Users will now show a connection status of Active. At this point all of the optional configuration items available under the System Admin tab will be displayed.
Advanced Configuration - System Admin Tab

Once basic configuration is complete, the following additional configuration groups become available. A brief description of each of this follows, with detailed information on configuration and usage provided in the indicated sections of this guide.

Mail Settings

BlackShield ID uses email for a variety of purposes including:

- Administrative alerts related to system events (refer to Events and Alerts on page 74).
- Authentication policy exceptions (refer to Authentication Thresholds Group on page 85).
- Token provisioning and user self-enrollment (refer to Self-Enroll Function and Rule-based Provisioning on pages 116 and 120 respectively).

![Figure 18 – Mail Settings](image)

Configure Mail Settings

- **From Address**: This value identifies messages as coming from BlackShield ID. In the example above, messages sent by BlackShield ID will appear to be From: BlackShield ID Mailer (admin@localdomain.ma...). You can modify these values to reflect the "From" name and address of your choice, provided that the email address is valid on your mail server.
- **SMTP Server**: This defines the mail server to be used by BlackShield ID for sending messages and alerts. This should be a resolvable name or IP address to a working SMTP (mail) server.
- **SMTP User**: If your mail server requires authentication, enter a valid user name in this field.
- **SMTP Password**: This is the password that corresponds to the SMTP User account.

Use the **Test** button to send a test message to the address configured in the "From Address" field.

Click **Apply** in the Actions Group to save changes to this section.
SMS Settings

BlackShield ID can send passcodes to users via SMS (refer to SMS/OTP Zero footprint tokens on page 111). To do so the server must be configured to connect to a public SMS gateway or to a local SMS modem.

SMS Gateway

Currently BlackShield ID can be configured to use the following public SMS Gateways:

- AQL (http://www.aql.com)
- CellTrust (http://www.celltrust.com)
- Clickatell (http://www.clickatell.com)
- TynTec (http://www.tyntec.com)

To use either of these gateways you must become a subscriber of their service. For other gateways contact CRYPTOCard Professional Services.

SMS Modem

An alternative to using an SMS gateway is to purchase a SMS modem and install a SIM card from a mobile phone account with sufficient SMS messaging capacity to accommodate your requirement. The number of messages per minute that can be sent is a function of the modem.

Keep in mind that messages/minute may not be a significant factor in determining which modem to use. If your service is configured for SMS/OTP on demand, then your users will require immediate delivery of an SMS/OTP. In this case, peak loading should be used to determine the required SMS throughput.

In a default configuration, BlackShield ID automatically sends an SMS/OTP immediately following a successful logon, so that it is available on the mobile device in advance of the next logon attempt. This means that if a user is not likely to log on again for 2 hours, the modem throughput need only be sufficient to ensure that the SMS/OTP is delivered before 2 hours elapses since the last logon.

The following SMS modems with USB interfaces have been extensively tested with BlackShield ID:

- Sierra Wireless (formerly Wavecom) Fastrack modems
- MultiTech Systems MultiModem GPRS

The above modems can be attached to a BlackShield ID server using a USB interface. For redundancy a second modem can be attached to a second BlackShield ID server.

BlackShield ID can address a remote SMS modem using telnet. This functionality has been tested with the MultiTech MultiModem GPRS.
Configuration

Each of the above SMS options has the following configuration items in common:

**OTPs per SMS**: This setting determines the number of OTPs sent with each message. By default this value is 1. This value can be increased to 5 OTPs/message.

**Resend OTP(s) on Challenge**: This feature allows a user to request an OTP by supplying a blank or single character password during login.

**Request Interval**: The amount of time a user must wait before they can request an additional OTP.

**Challenge Time to Live**: The amount of time the OTP remains valid, if exceeded; the user must request a new OTP.

You should select “5” OTPs per SMS if your SMS service is configured to deliver SMS/OTPs after each successful logon and there is a high probability that users will frequently be in locations not capable of receiving an SMS.

The Phone Number field can be used in conjunction with the Test button to verify the configuration by sending an OTP to the indicated number. The format of the number must be country code followed by city code, followed by the number.

Example 1: North American numbers would be in the format: 12128881111 where 1 is the country code, 212 is the city code and 8881111 is the local number.

Example 2: UK numbers would be in the format: 447815232134 where 44 is the country code, 7815 is the city code and 232134 is the local number.

To configure SMS gateways or modems click the “Configure” button.
Configuring AQL SMS Gateway

Select AQL from the SMS Settings dropdown list.

Select the BlackShield ID site that will use this SMS gateway from the Site dropdown.

Enter the username, password and SMS URL of your AQL account.

If a proxy is being used, select the proxy radio button and input the proxy server information.

Select the Send Flash SMS Message option if you want the SMS message to appear directly on the phone's screen, instead of the 'Inbox'. The recipients phone must support this functionality.

Click Save to update the configuration.

The service configuration is updated. It is now possible to test the service by inputting a valid SMS number and clicking the Test button.

Configuring CellTrust SMS Gateway

Select CellTrust from the SMS Settings dropdown list.

Select the BlackShield ID site that will use this SMS gateway from the Site dropdown.

Enter the username, password, SMS URL, Nickname and Carrier ID (optional) of your CellTrust account.

If a proxy is being used, select the proxy radio button and input the proxy server information.

Click Save to update the configuration.

The service configuration is updated. It is now possible to test the service by inputting a valid SMS number and clicking the Test button.
Configuring Clickatell SMS Gateway

Select Clickatell from the SMS Settings dropdown list.

Select the BlackShield ID site that will use this SMS gateway from the Site dropdown.

Enter the username, password, SMS URL and API ID of your Clickatell account.

If a proxy is being used, select the proxy radio button and input the proxy server information.

Select the Send Flash SMS Message option if you want the SMS message to appear directly on the phone's screen, instead of the 'Inbox'. The recipients phone must support this functionality.

Click Save to update the configuration.

The service configuration is updated. It is now possible to test the service by inputting a valid SMS number and clicking the Test button.

Configuring TynTec SMS Gateway

Select TynTec from the SMS Settings dropdown list.

Select the BlackShield ID site that will use this SMS gateway from the Site dropdown.

Enter the username, password, SMS URL and Sender ID of your TynTec account.

If a proxy is being used, select the proxy radio button and input the proxy server information.

Click Save to update the configuration.

The service configuration is updated. It is now possible to test the service by inputting a valid SMS number and clicking the Test button.
Configuring SMS Modem (Local)

Insert a SIM card for a mobile phone account with SMS capability into a SMS – GSM modem. Ensure that the modem is properly configured for your country.

Select SMS-GSM Modem Plug-in from the dropdown list.

Select the Send Flash SMS Message option if you want the SMS message to appear directly on the phone's screen, instead of the 'Inbox'. The recipients phone must support this functionality.

Click Save to update the configuration.

The service configuration is updated. It is now possible to test the service by inputting a valid SMS number and clicking the Test button.

Configuring SMS Modem (Remote)

Insert a SIM card for a mobile phone account with SMS capability into a SMS – GSM modem. Ensure that the modem is properly configured for your country. The modem must be configured to accept commands without requiring authentication.

Select SMS - Telnet Modem Plug-in from the dropdown list.

Enter the Host name or IP address and the port number for the system hosting the remote modem.

Select the Send Flash SMS Message option if you want the SMS message to appear directly on the phone's screen, instead of the 'Inbox'. The recipients phone must support this functionality.

Click Save to update the configuration.

The service configuration is updated. It is now possible to test the service by inputting a valid SMS number and clicking the Test button.
Agent Settings

BlackShield ID agents send authentication requests to BlackShield ID. Security sensitive data sent between the server and agents is protected by AES 256 encryption. To encrypt the traffic and to prevent unauthorized agents, BlackShield ID requires that each server and each agent use an identical encryption key file.

A default encryption key file is automatically installed with the server and with each agent. For optimum security a new encryption key file should be created and used to replace all default encryption key files.

For information on individual agents and configuration refer the corresponding installation and implementation guides included with the BlackShield ID Authentication Platform distribution or available for download from blackshieldid.cryptocard.com

Generate Agent Encryption Key File

Click Configure in the Agent Settings Group.

To create a new encryption key file Click Create New. Save the file to a secure location. Use this file to replace the key file at each installed agent.

Assuming default installation, the location of the key file for each agent is in Key File folder. Using the IIS 6 Agent as an example, the default location would be \Program Files\CRYPTOCARD\BlackShield ID\IIS Agent\KeyFile\default.BlackShield ID key.

Each time a key file is generated the Previous Keys list is updated. To fallback or recreate a previous key, select it from the list then click the Restore button. Save the file to a secure location and use the file to replace all existing agent and server key files.
The BlackShield ID IIS application pool must be restarted to begin using the new encryption key file.

Self-enrollment and Self-Service Sites

By default, web sites that support self-enrollment and user self-service are created on the web server hosting BlackShield ID during installation. Self-enrollment is used to aid in transparent migration of users from passwords or other authentication methods and to increase the efficiency of token provisioning. Self-service allows users to request a new SMS/OTP, resynchronize tokens and perform on-demand PIN changes without the assistance of the Security Administrator.

Self-enrollment group

This group is used to configure the location of the self-enrollment site as well as a number of security and management by exception alerts.

Base URL: this is the location of the site and will form part of the URL included with each self-enrollment notification. The default location is the BlackShield ID server. If a remote self-enrollment site has been created, this value should reflect the URL of the remote site.

Self-enrollment over SSL If this box is checked, enrollment must take place over SSL. To use SSL a valid certificate must be installed on the localhost and the Base URL should be modified to https.

Activation Code This is a unique security code for each user that is required to complete self-enrollment. The format of this code can be numeric, alphabetic or alphanumeric as selected in the dropdown.

Reservation Time to Live This is the maximum number of days allowed to complete the self-enrollment process from the time a token is issued. BlackShield ID issues a Security Administrator alert if this threshold is exceeded. If set to 0, the reservation does not expire.
Enrollment lockout after

This setting limits the number of enrollment attempts per user. BlackShield ID issues a Security Administrator alert if this threshold is exceeded and deletes the enrollment URL. The Security Administrator can complete the enrollment process for the user from the Secured Users Tab.

Set assigned tokens to lost

This value determines the number of days after the reservation time to live expiration allowed before BlackShield ID marks the un-enrolled token as lost. This removes the un-enrolled token from the user and includes a history notation reflecting the cause for this action.

Click Apply in the Actions group to save configuration changes to this group.

Self-service group

This group is used to configure the location of the Self-service site.

By default this is a site on the BlackShield ID server.

Figure 19 - Self-Server / Self-Enroll Default Install

If a remote Self-service site has been installed, the URL must be updated to reflect the new location.

Click Apply in the Actions group to save configuration changes to this group.

Remote Services Setting

In large installations or for improved performance and security, it may be desirable to separate self-enrollment and/or self-service web sites from the BlackShield ID server, including placing a firewall between these sites and the server.
As with agents, BlackShield ID requires that these remote web sites/services use a service encryption key to protect the transferred data.

BlackShield ID enrollment and self-service remote sites send authentication requests to BlackShield ID. Security sensitive data sent between the server and remote sites is protected by AES 256 encryption. To encrypt the traffic and to prevent unauthorized sites, BlackShield ID requires that each server and every remote site use an identical encryption key file.

A default encryption key file is automatically installed with the server and with each site. For optimum security a new encryption key file should be created and used to replace all default encryption key files.

**Generate Remote Service Encryption Key File**

Click Configure in the Remote Services Settings Group.

To create a new encryption key file Click Create New. Save the file to a secure location. Use this file to replace the key file at each installed agent.

Each time a key file is generated the Previous Keys list is updated. To fallback or recreate a previous key,
select it from the list then click the Restore button. Save the file to a secure location and use the file to replace all existing Service and server key files.

For information on installing and configuration enrollment or self-service refer to Self-enrollment and Self-Service Sites on page 71.

Events and Alerts

The monitoring service installed with BlackShield ID monitors the system for events and security policy threshold exceptions which may result in the authentication service being degraded or cause a delay or disruption of service if not addressed.

All alert notifications are sent by email to the recipients configured in this section.

Refer to Mail Settings on page 64 for email server configuration instructions.

Configure Events and Alerts

E-mail

Use this field to add recipient email addresses to the events and alerts recipient list by entering the address and clicking the Add button.

Alert Recipients

Lists all addresses configured to receive events and alerts. To remove an address highlight it then click the Remove button.

Check the following events to add to the event and alert notification

Service Not Responding

This selection captures events such as loss of connection between the database, directory and server.

Alert Operator on enrollment lockout

Relates to self-enrollment and the “enrollment lockout after” threshold. Refer to Self-enrollment group on page 71.
Alert Operator on expired reservation: Relates to self-enrollment and the “Reservation time to live” threshold. Refer to Self-enrollment group on page 71.

Low disk space Generates an alert if available disk space falls below the configured threshold.

License capacity Generates an alert if the available capacity falls below the configured threshold.

Alert Operator on orphaned token Generates an alert if a token is de-assigned from a user created in the internal SQL database as a result of a duplicate UserID found in LDAP.

License expires Generates an alert if an evaluation, temporary or time-limited license will expire within the configured threshold.

Logging

In addition to databasing authentication history and Security Administrator activity, BlackShield ID also logs authentication activity and system events. Logs can be created for viewing in Event Viewer or stored locally in a tab delimited file.

Use of Event viewer is recommended if you are currently using a reporting tool that can parse event viewer logs, otherwise the tabbed log file is recommended. The recommended logging level is Default. This captures detail that is sufficient for audit and most troubleshooting purposes. High should only be used when advised by CRYPTOCard or your supplier. High captures detail that may be useful for fault resolution in uncommon circumstances.

Log files are created if activity occurs on the server and appended to a log file. The date of the event is compared with the current log file date. If the dates match, the event is appended to the current log file. If the event date is greater than the current log file date, a new log file is started. All log files have names in the format of BlackShield Log – 20090708.log where the digits indicate the event dates captured in the log file.

Assuming a default installation, log files are located in: \Program Files\CRYPTOCARD\BlackShield ID\Log and have a .log extension and include the date in the file name.

For a description of the other folders and files contained in the Log directory refer to On-line Reports on page 163.
Archiving

BlackShield ID stores virtually all server activity in the database, including authentication history, token provisioning tasks, User management and Security Administrator activity. Over time this can cause the database to become very large.

The archiving function removes old activity records from the database and writes these records to comma separated files on the server. This preserves the data which can be imported into commonly available reporting tools as required while keeping the amount of data stored in the database to an optimum level.

All archive files have the format yyyymmdd_Range_yymmdd-yyyyymmdd.csv where yyyymmdd represents the date the archive was created and Range_yymmdd-yyyyymmdd represents the date range of the records included in the archive.

Archive Configuration

- **Number of rows allowed**: sets the maximum number of rows allowed for activity history in the database. The oldest records that exceed this threshold are archived.

- **Number of days allowed**: sets the maximum age of activity history in the database. Records that are older than the threshold are automatically archived.

- **Archiving Site**: sets the BlackShield ID site to which records will be archived.

Assuming a default installation, records are archived to one of the sub-folders in the \Program Files\CRYPTOCARD\BlackShield ID\Log folder on the target BlackShield ID server.

Auth Archive

This folder is the archive for authentication history records. The comma delimited data corresponds to:

- SystemID, UserName, Organization, Serial, Activity Date, Action, Result, IP, Agent ID, Message, Site Host, Used Name.

Operator Archive

This folder is the archive for Operator (Security Administrator) history records. The comma delimited data corresponds to:
System ID, User Name, Organization, Activity Date, Action Class, Action Type, Action Result, Action Data.

Token Archive

This folder is the archive for Token state and usage history records. The comma delimited data corresponds to:

Action, Serial, User Name, Organization, Template ID, State, State set date, Last Auth Date, PIN Set Date, Unlock At, In Service, In Service OP, Init Date, Display, OTP TTL, Auth Attempts, Activation Count, Challenge Issued, Last Use, Modified Date, Modified By, Message, System ID.

User Data Archive

This folder is the archive for User account management and attribute history records. The comma delimited data corresponds to:

Action, User Name, Unlock At, Start Date, End Date, Start Time, End Time, Restricted Days, Message, Temporary Password, Password Change Req., Password Set Date, Password Attempt Count, Created Date, Created By, Modified Date, Modified By, System ID, Organization.

Users Archive

This folder is the archive for User account management and attribute history records. The comma delimited data corresponds to:

SystemID, UserName, Organization, Serial, Activity Date, Action, Result, IP, Agent ID, Message, Site Host, Used Name.

Visual

The visual group is used to upload an image to BlackShield ID that replaces the default CRYPTOCard logo visible in the upper left corner of the manager UI. Any image that corresponds to 162 x 40 pixels in the .gif format is acceptable.

Provisioning Rules

Provision rules represent one of 3 ways to automate token provisioning and workflow. For this reason the application and configuration of Provisioning Rules Settings is covered in Rule-based Provisioning on page 121.
Pre-Authentication Rules

PreAuth is arguably the most powerful function of BlackShield ID. It allows Security Administrators to create rules by which User attributes are evaluated and only if the evaluation is True will authentication proceed. Pre-Authentication rules are covered in PreAuthentication Rules on page 132.
Chapter 7 – Security Policy

In this chapter:

- Security policy
- Token templates
- Synchronization
- Server-side PIN Policy
- Temporary password policy
- Access restrictions
- Token file creation
- Token file location
- Third Party Authentication Options

Policy Admin Tab

The Policy Tab groups most functions that relate to the overall security policy of the server. Its purpose is to provide a flexible and convenient way to tune the server to meet your organizations security policy. Through settings on this tab, you can place limits on Operator functions, enforce a consistent authentication process and user logon experience and protect against denial of service, brute force and other account credential attacks.
Token Templates

Token templates apply the operating characteristics such as passcode strength to be applied to all tokens of a given type during initialization. A template modification does not affect tokens that are already initialized and does not affect issued tokens. To make existing tokens conform to a new template, it is necessary to reinitialize the token. Token Templates are provided for KT, RB, MP, SMS, 3rd party OATH, GrIdsure and legacy 6.x legacy, 5.x legacy and 4.x software tokens.

The options presented in a template vary depending upon the token type. In addition, the selection of one option may preclude the availability of another option. All possible options are described below and apply to all token types unless otherwise noted.

To view or modify an existing template, select the token type from the drop down and click ‘Edit’. The Edit Token Template dialogue is displayed.

Passcode Policy Group

By default all tokens use AES 256 bit encryption. Certain 3rd party tokens use 3DES or OATH. BlackShield ID automatically applies the strongest algorithm supported by the token type.

The options available within each policy vary based on token type.

Mode: Tokens can operate in either Challenge-Response or Quick Log mode. Default value: Quick Log.

Quick Log mode is recommended because it greatly simplifies the User logon experience and strengthens security by eliminating the requirement to have the user key a challenge.
into a token to get an OTP.

**Complexity:** The OTPs generated by the token can be comprised of numbers, letters and additional characters as follows:

- **Decimal:** token generates passcodes comprised of digits from 0-9.
- **Hexadecimal:** token generates passcodes comprised of digits and letters from 0–9 and A-F.
- **Base32:** token generates passcodes comprised of digits and letters from 0-9 and A-Z. (Default value).
- **Base64:** token generates passcodes comprised of digits and letters from 0-9 and Aa-Zz, as well as other printable characters available via Shift + 0-9.

**Length:** This option determines the number of characters displayed as the OTP. Options are 5, 6, 7 or 8 characters. Default value: 8.

**Display Mask:** if set to ‘Telephone Mode’, the 4th character of the OTP will always be a dash (“-“). Typically this is used with a decimal OTP, length of 8. Example OTP: 123-5678. If set to ‘None’, the 4th character is unmodified. Example OTP: 12345678. Telephone mode can be used with any token complexity and length setting. Default value: None. Note the dash is not entered as part of the OTP on login attempts.

**Passwords/Cycle:** This option is used in conjunction with Operation Policy (Manual Shut-Off, Auto Shut-Off). Tokens can be limited to generating 1 password per cycle or allow multiple passwords to be generated in a cycle. Default value: Single.

- For tokens with a ‘No PIN’ or ‘Server-side’ PIN policy, the selection of Single in combination with Manual Shut-Off set to Disabled means that the token will not generate another password until the Auto Shut-Off value has expired. For example, if the value is 60 seconds, the user must wait 60 seconds before another password can be generated.
- For tokens with a ‘Fixed’ or ‘User selected’ PIN, selection of Manual Shut-off set to Disabled means that the token will not generate another password until the Auto Shut-Off value has expired and the user enters their PIN into the token.

**Operation Policy Group**

**Manual Shut-Off:** If ‘Enabled’, the user can clear the OTP from the display and turn the token off at any time by pressing the appropriate button, depending on the token type. If ‘Disabled’, the OTP will be displayed until the Auto Shut-off value expires. Default Value: Disabled.

**Auto Shut-Off:** This value determines the length of time the password will be displayed, 30, 60 or 90 seconds. On expiration of this value, the token automatically clears the display and shuts off. Default Values: 60.
NOTE: CRYPTOCard recommends using the Operation Policy Group default settings for tokens configured for QUICKLog operation. Doing so ensures that the user must wait at least 60 (default) seconds before the token will generate another passcode.

PIN Policy Group

PIN Type: This setting determines the type of PIN to be used with the token:

- **No PIN** means that the user will not use a PIN. The token generated password will be sufficient for authentication.

- **Fixed PIN** means that the PIN generated for the token during initialization is permanent and cannot be changed without reinitializing the token. This PIN must always be keyed into the token before a password is generated.

- **User selected PIN** means that the user must change the PIN generated for the token during initialization before a password will be generated. Thereafter the user can change the PIN at any time. Note that the PIN change must conform to the minimum requirements for PIN Length, Complexity and Maximum PIN Attempts.

- **Server-side Fixed** means that the PIN generated for the token at initialization is permanent and cannot be changed without reinitializing the token. This PIN type is evaluated at BlackShield ID.

- **Server-side User Select** means that the PIN generated for the token can be changed by the User. The new PIN must conform to the minimum requirements set in the Server-side PIN Policy Group on the Policy Admin Tab. Refer to Server-side PIN Policy on page 86.

Server-side Server Select means that the PIN generated for the token can be changed however the new PIN will be generated by BlackShield ID and will conform to the minimum requirements set in the Server-side PIN Policy Group on the Policy Admin Tab.

Note: Server-side PINs require the user to prepend the PIN to the OTP generated password during login, allowing the PIN to be evaluated by BlackShield. For example, if the user PIN is ABCD and the OTP is 12345678, the user would enter ABCD12345678 at the password prompt. All other PIN types require the user to key the correct PIN into the token before an OTP is generated. In this case the user provides only the OTP at the password prompt. For example, if the user PIN is 8432 and the OTP is 12345678, the user will enter 12345678 at the password prompt. Generally Server-side PINs are used with KT tokens.

- **Initial PIN**: determines the nature of the initial PIN created for a token during initialization. If ‘Random’, BlackShield ID will generate a random PIN that conforms to the minimum PIN Policy options set in the dropdowns for this group for each token during initialization. If ‘Fixed’, all tokens will be initialized with the same PIN. Default value: Random.

- **Min. PIN Length**: determines the minimum PIN length that can be used with the token.

- This option is disabled if PIN Type is set to ‘No PIN’. The user will not be required to use a PIN at any time.
This option is disabled if PIN Type is set to Server-side Fixed, Server-side User Select or Server-side Server Select. The user will be required to use a PIN according to the options set in the Server-side PIN Policy Group.

This option is enabled if PIN Type is set to Fixed PIN or User selected PIN. This requires that any PIN set for the token meet the indicated minimum number of digits. The range is 1 to 8 digits.

**Allow Trivial PINs:** If enabled, a PIN may be 3 or more consecutive numbers (i.e. 1234) or 3 or more identical digits (i.e. 2222). Default value: cleared.

**Max. PIN Attempts:** determines the maximum number of consecutive failed PIN attempts permitted by the token. If this number is exceeded, the token will enter the ‘Locked’ state and cannot be used for authentication until it is reinitialized. This option is available only if PIN Type is set to Fixed PIN or User selected PIN.

Click the ‘Apply’ button to apply changes to the template. Changes to the template will be applied to their respective token types during initialization. Previously initialized tokens will be unaffected by changes to a template.

**Third Party Authentication Options**

**Grid Size:** determines the size of the Gridsure grid displayed to the user during authentication.

**Synchronization**

The Synchronization group applies only to tokens configured for “QUICKLog” event-synchronous authentication.

Tokens configured for QUICKLog do not rely on time to remain synchronized with the server, avoiding the problems of time drift common with large deployments of “Time-synchronous” tokens. Instead, each time the token is activated, a new tokencode is generated. For each logon “event” the server compares the submitted passcode with the expected passcode. Occasionally a user may generate a passcode without using it, causing the token to be “ahead” or out of sync with the server during the next logon.

The Synchronization Window settings provide a secure mechanism through which the server and token can automatically resynchronize during logon and in the process, discard any unused passcodes.

<table>
<thead>
<tr>
<th>Synchronization</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Inner event based OTP window size</td>
<td>10</td>
<td>(1 - 99)</td>
</tr>
<tr>
<td>Outer event based OTP window size</td>
<td>100</td>
<td>(1 - 3,600)</td>
</tr>
</tbody>
</table>
Inner OTP synchronization window size

This represents the number of passwords the server will “look-ahead” from the last successful logon by the user. Using the example above, the server would be expecting passcode number 1 though the user provides passcode number 2. Assuming the default inner window value of 3, the server would look from passcode 1 to 3 until a match is found (in this case at passcode 2). If a match is found, the user is authenticated and any unused passcodes are discarded. The next valid passcode on the server would be passcode 3. Default value: 3.

Outer OTP synchronization window size

This handles situations where the user’s passcode is not found in the inner window. In this case, the server will look ahead up to the indicated value (by default 100). If a match is found in this window, the user is prompted to provide the next passcode in sequence. For example, if the user provides passcode 4, the user will be prompted for and must provide passcode 5. In essence this window has an effective size of 1. Default value: 100.

Click ‘Apply’ in the Actions group to apply changes to these values.

Authentication Thresholds Group

Authentication thresholds determine how the server handles failed authentication attempts. It is a useful tool for mitigating account brute force and DOS attacks, providing early warning of an attack and at the same time, minimizing the impact on Operators and Help Desks.

Account Lock threshold

This determines the maximum number of consecutive failed logon attempts permitted by the system. If this threshold is exceeded, the user account is locked. If this value is set to 0, the account will not be locked. Default value: 3
Alert Operator on Account Lockout

If this option is checked, an email alert will go to all addresses in the Alert Recipients List (System Admin Tab). The text of this email alert can be modified by editing the OperatorLockoutAlert.emt file. Refer to Section EMT File List on page 184 for more information. Default value: cleared.

Alert User on Account Lockout

If this option is checked, an email alert will go to the users email addresses. The text of this email alert can be modified by editing the UserLockoutAlert.emt file. Refer to Section EMT File List on page 184 for more information. Default value: cleared.

Account Lock Duration

This option determines the period of time the account will remain locked. When this threshold is exceeded, the account will automatically unlock and the user will be able to logon. If this value is set to 0, the account will not unlock automatically. The value may be Seconds, Minutes, or Hours, with the allowed range of 0 to 99. Default value: 15 Minutes.

Alert Operator on Account Unlock

If this option is checked, an email alert will go to all addresses in the Alert Recipients List (System Admin Tab) when this account becomes unlocked. The text of this email alert can be modified by editing the OperatorUnlockAlert.emt file. Refer to Section EMT File List on page 184 for more information. Default value: cleared.

Alert User on Account Unlock

If this option is checked, an email alert will go to the users email addresses when this account unlocks. The text of this email alert can be modified by editing the UserUnlockAlert.emt file. Refer to Section EMT File List on page 184 for more information. Default value: cleared.

Click ‘Apply’ in the Actions group to apply changes to these values.

Server-side PIN Policy

This group sets a global PIN policy that will be applied to all tokens initialized with a Server-side PIN. Policies set in this section cannot be overridden by Operators that do not have access to the Policy Admin
Tab. Changes to this policy are immediate. Click ‘Apply’ in the Actions group to apply changes to these values.

**Figure 38 - Server-side PIN Policy**

**Change PIN on first use required**

This option forces the user to change the initial PIN set for the token during initialization or set by an Operator before they can logon. For example, if the initial PIN is ABCD and the password is 12345678, the user will attempt to logon with ABCD12345678. Assuming this combination successfully authenticates against BlackShield ID, the user will then be prompted to change their PIN to a new value that meets the minimum requirements of the Server-side PIN Policy and known only to them. If this option is checked, the Operator cannot override this policy. If this option is cleared, the Operator can choose whether or not to force a PIN change on first use. Default value: checked.

**Force Random PINs**

This causes BlackShield ID to generate random PINs for each user that meets the Server-side PIN policy requirements. If checked, the Operator cannot choose or enter a PIN. If cleared, the Operator can create a PIN or request a PIN be generated by BlackShield ID. Default value: checked.

**Minimum Length**

This sets the minimum PIN length that may be set. Range is 3 to 15 characters. Default is 3 characters.

**Maximum Length**

This sets the maximum PIN length that may be set. Range is 4 to 16 characters. This value must be greater than or equal to the minimum length. Default value is 8 characters.

**Minimum Complexity**

This determines the combination of characters that must be used in a PIN. Default value: Complex alphanumeric
• Numeric: the minimum requirement is a PIN comprised of digits 0-9.
• Alphanumeric: the minimum requirement is a PIN that contains at least 1 digit and 1 upper case letter. 0-9, A-Z
• Strong Alphanumeric: the minimum requirement is a PIN comprised of at least 1 digit, 1 upper case letter and 1 lower case letter. 0-9, Aa-Zz.
• Complex alphanumeric: the minimum requirement is a PIN comprised of at least 1 digit, 1 letter and 1 special character. 0-9, Aa-Zz, &^%$ and other printable characters.

Change Frequency

This determines how frequently a user will be required to change their Server-side Server Select or Server-side User Select PIN. This period commences with the last PIN change date for a token. Default is 30 days.

Random PIN Length

This determines the PIN length generated by BlackShield ID for server-generated PINs.

PIN Change Exclusion List

Though uncommon, there are a few RADIUS clients that have not implemented the full RADIUS specification and as a result do not support PIN change. This can result in a failed logon if the server attempts to enforce a PIN change policy during logon through a non-compliant RADIUS client. This setting allows the IP address of the non-compliant RADIUS client to be added to a PIN change exclusion list. BlackShield ID will not enforce a required PIN change for any RADIUS client in the list.

Enter the IP address of the non-compliant RADIUS client in the ADD a New IP field, and then click Add.

To remove an IP address, highlight it in the list and click Remove.

Temporary Password Policy

This section applies to temporary static passwords assigned to user accounts through BlackShield ID. As with Server-side PIN Policy, these Options set global policy, apply to all users and cannot be overridden by Operators that do not have access to the Policy Tab. Click ‘Apply’ in the Actions group to apply changes to these values.
Figure 39 - Temporary Password Policy

Temporary password Allowed

This option determines whether a static password can be assigned by BlackShield ID. When checked, an Operator can assign a temporary password to a user, provided the user does not currently have an active token. If cleared, Operators may not assign a temporary password to a user. Default value: checked.

Change Password on first use required

This option forces the user to change the static password assigned by an Operator before they can logon. The user must first provide a valid password and then is prompted to replace the password. If this box is checked, all users assigned a static password will be required to change it on first use. The Operator cannot override this policy. If cleared, the Operator has the option of requiring a password change on first use. Default value: checked.

Minimum Length

This is the minimum length password that BlackShield ID will allow. Range is 3 to 15 characters. Default value: 8.

Maximum Length

This is the maximum length password that BlackShield ID will allow. Range is 4 to 16 characters. This value must be greater than or equal to the minimum length. Default value is 16 characters.

Minimum Complexity

This determines the combination of characters that must be used in a password. Default value: Complex alphanumeric.

- Numeric: the minimum requirement is a password comprised of digits 0-9.
• Alphanumeric: the minimum requirement is a password that contains at least 1 digit and 1 upper case letter. 0-9, A-Z.
• Strong Alphanumeric: the minimum requirement is a password comprised of at least 1 digit, 1 upper case letter and 1 lower case letter. 0-9, Aa-Zz.
• Complex alphanumeric: the minimum requirement is a password comprised of at least 1 digit, 1 letter and 1 special character. 0-9, Aa-Zz, &^%$ and other printable characters.

Change Frequency

This determines how frequently a user will be required to change their static password. This period commences with the last static password change date for a token. Default value: 30 days.

Force Random Passwords

This determines whether an Operator can choose the password to be given to a user. If cleared the Operator can manually create or request BlackShield ID to create a password that conforms to the policy. If checked, BlackShield ID will generate a password and the Operator that does not have access to the Policy Tab will not be able to override this policy. Default value: cleared.

Force Maximum Lifetime

This determines how long a temporary password will remain active. Default value: disabled.

Authentication Policy

Allow case insensitive hexadecimal responses. Default value: disabled. By default, the server will expect all hexadecimal responses to be uppercase.

The number of disconnected authentications the token can perform when disconnected from the network, in the range 2 to 100. In essence, this is the number of predefined hashes transferred from the server to the client for use when the client is no longer connected to the network. After configuring the number of disconnected authentications, the user must perform an online authenticated logon to the machine in question at least once before a disconnected logon can be performed. This setting is used by the BlackShield ID Windows Logon package.
Restrictions Group

BlackShield ID supports the application of access restrictions when assigning a token or static password to a user. Access restrictions can be used to limit when a user’s right to authenticate by date range (i.e. January 1, 2007 to December 31, 2008), day of week (i.e. Monday-Friday only) and time of day (09:00 – 17:00 only). Refer to Access Restrictions on page 118.

If checked, Operators can assign access restrictions. If cleared, access restrictions cannot be applied. Default value: checked.

Click ‘Apply’ in the Actions group to apply changes to these values.

Token File Creation

By default BlackShield ID issues MP software tokens, which uses AES 256-bit encryption to generate passcodes. Changing this selection will cause the server to generate tokens that are compatible with older or deprecated software tokens. CRYPTOCard strongly recommends the MP token and advises that support for older or deprecated versions will be dropped from BlackShield ID in future releases.

Allowed Targets Settings (Settings)

The Allowed Targets Settings dialog allows you to specify installation targets and custom messages when performing Self Enrollment of MP tokens.
Allowed Target Settings

General Settings

- Allows users to edit phone number and email address during Self Enrollment rather than using the default information configured within BlackShield ID for each user.

Settings

- Require phone description
- Show MP token target selector as drop-down list
- Allow Install Locally
- Allow Smart Card
- Allow Secure Flash Drive
- Allow Java Enabled Phone
- Allow Blackberry
- Allow iPhone

MP Token Targets

<table>
<thead>
<tr>
<th>Target Location</th>
<th>Target Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Install Locally</td>
<td>Install Locally</td>
</tr>
<tr>
<td>Smart Card</td>
<td>Smart Card</td>
</tr>
<tr>
<td>Secure Flash Drive</td>
<td>Secure Flash Drive</td>
</tr>
<tr>
<td>Java Enabled Phone</td>
<td>Java Enabled Phone</td>
</tr>
<tr>
<td>BlackBerry</td>
<td>BlackBerry</td>
</tr>
<tr>
<td>iPhone</td>
<td>iPhone</td>
</tr>
</tbody>
</table>

Figure 26 – Allowed Target Settings (Settings)

General Settings

- Allows the user to edit their phone number and email address during Self Enrollment rather than using the default information configured within BlackShield ID for each user.

Settings

- Allows the control of the target location when a user is installing an MP token, the selections include: Install Locally (hard drive), Smart Card, Secure Flash Drive (IronKey® and SafeStick®), Java Enabled Phone and BlackBerry. If custom phone messages were created for Java enabled phones (configured in the Devices section of the Allowed Targets dialog), select the “Show MP token target selector as a drop down list” option.

MP Token Targets

- Allows custom text for each MP target location specified in the MP Token Targets section.
Allowed Targets Settings (Devices)

The Devices section allows the creation of custom target location dialogs displayed during Self Enrollment. The dialogs will appear after the user has selected the target location.

![Allowed Target Settings (Devices)](image1)

**Figure 27 – Allowed Target Settings (Devices)**

New Device

Selecting New Device will display a custom text configuration dialog. Customizing the Title, Description, Download Notes, Removal Message and Target Location Type are available.

![Allowed Target Settings (New Devices)](image2)

**Figure 28 – Allowed Target Settings (New Devices)**

This section should be used if third party software is needed to activate an MP token on a Java enabled phone, although it can be used for any other target type. If no custom device messages are created or they do not apply to the target installation type, the default Self Enrollment dialogs will appear.
Token File Location Group

BlackShield ID allows Legacy software tokens generated on version 4, 5 and 6 servers to be issued to users. This group is used to define the default location for these token files. The Operator must have write permissions to the selected directory path for the token to be issued successfully. The path entered will also be local to the BlackShield ID unless a network path is entered.

Third Party Authentication Options

This section applies to the default behaviour of a GrIDsure token.

![Third Party Authentication Options](image)

**Figure 29 – Third party Authentication Options**

**Allow trivial PIP’s:**

A PIP (Personal Identification Pattern) may consist of a diagonal line, straight line, or the four corners of the grid. Default value: cleared

**Use Numbers**

If enabled, display numbers within a GrIDsure grid (0-9). Default value: selected

**Use special symbols/characters**

If enabled, allows special symbols/characters within a GrIDsure grid ( !@#$%^&*? ). Default value: cleared

**Use uppercase letters**

If enabled, displays characters in uppercase within a GrIDsure grid (A-Z). Default value: cleared

**Use lowercase letters**

If enabled, displays characters in lowercase within a GrIDsure grid (a-z). Default value: cleared
Chapter 8 – Token Management and Provisioning

In this chapter:

- Importing factory programmed tokens
- Initializing RB and KT series tokens
- Creating Software tokens
- Issuing tokens
- Self-enrollment
- Temporary Passwords

Assignment Tab

The Assignment Tab is designed for use by Security Administrators. It groups functions that relate to managing token inventory and manual assignment of tokens to users. In general, Help-desk functions related to managing users that have already been assigned tokens and/or are allowed to authenticate against BlackShield ID are grouped on the Secured Users Tab. A number of functions are common to both tabs.
Assignment Search / Users: Containers

BlackShield ID retains the organization of users as they exist in LDAP containers and as they’ve been organized in the internal database (Containers Tab on page 138). To drill down and refine the users list to users from a specific container, simply click on the container. Use the up arrow to navigate up the container hierarchy.

Figure 30 – Assignment Tab
Assignment Search / Users: Assignment Search Group

The Assignment Search Group provides the ability to search for users using a variety of criteria. The search function supports '*' wildcards and minimum matching. For example: bro, bro*n will find Brown and Browne while bro*ne will not find Brown.

- **Last Name**: Searches the ‘Last Name’ field
- **First Name**: Searches the ‘First Name’ field
- **User ID**: Searches the ‘User ID’ field

These fields may be combined in a single search. Click ‘Search’ to execute the search. Clear the search fields and click ‘Search’ to refresh the list of users in the Users Group.

- **Include Sub Groups**: When this box is checked the search function will search all Containers. If the box is not checked only the currently selected Container will be searched.

These fields may be combined in a single search. Click ‘Search’ to execute the search. Clear the search fields and click ‘Search’ to display all users in the Users Group.

![Assignment Search Group](image)

Figure 31 – Assignment Search Group

The results of the search are displayed in the Users Group.

**User**

This panel displays a list of users from all configured user data sources (LDAP / SQL) that meet the Assignment search criteria. The list can be sorted in ascending or descending order by clicking on any of the column headings. Clicking on a user will highlight the user and populate the User Detail Group and the Assigned Token fields.
User Detail

This panel is updated from LDAP or the internal SQL user data source whenever a user is highlighted in the Users list. It displays user detail as retrieved from LDAP or SQL along with all tokens assigned to the user. (Figure 31 on page 97)

- If the highlighted user is from an LDAP user data source, the displayed detail is read only. This is because BlackShield ID does not write to or modify LDAP.
- If the user is from the internal SQL user data source, the detail can be edited using the Add/Modify/Remove buttons in the User Mgt. group.

Figure 32 – User Detail Group

The custom 1, 2 and 3 fields are populated from LDAP based on custom mappings of these fields to LDAP objects as configured on the System Admin tab (System Settings: Users on page 54). To modify the Custom Field #1, Custom Field #2 and Custom Field #3 labels in this section, refer to Modifying Custom Fields on page 186.

Assigned Tokens Group

The Assigned tokens group displays all tokens assigned to the highlighted user.

Figure 33 - Assigned Tokens Group

The Revoke button is used to revoke the highlighted token. The revoke dialogue presents several options for managing the token after it is revoked. Refer to Revoking Tokens on page 128.
The Issue button is active for MP software tokens and is used during the manual assignment process to save the token initialization file or email it to BlackBerry users. Refer to Assign Software Tokens on page 110.

**User Mgmt Group**

BlackShield ID can concurrently support the authentication of users that are not in LDAP by allowing users to be added to its internal user database. This provides a convenient way for an organization to authenticate internal LDAP user accounts as while supporting authentication for users who are not in LDAP.

**Add a User to the internal SQL User Source**

To add a user to the internal SQL user data source:

1. Highlight SQL or a sub-container in the SQL user data source
2. Click the Add button in the User Mgt group.
3. The only required field is User ID, which must be unique across both the internal SQL user data source and LDAP.
4. An email address is required to enable the self-enrollment option for this user and to send any alerts for account lock/unlock (Authentication Thresholds Group on page 85).
5. Completing all fields is recommended.

**NOTE:** the Mobile phone number must be in the format of country code, city code, and local number and must only contain numbers if issuing SMS/OTP tokens. Incorrectly formatted numbers will prevent delivery of the SMS/OTP.
Edit or Remove a User from the Internal SQL user data source

Highlight the user in the user list. The Edit and Remove buttons in the User Mgt group will be enabled if the user is from the internal SQL user data source and does not have assigned tokens.

Overview of Token Management

All tokens to be managed by BlackShield ID must be added to the server inventory before they can be assigned to users. There are three ways to add tokens to inventory: Import, Initialization and Create.

Import

The import function is used to import factory programmed tokens into inventory. Factory programmed tokens do not require initialization to being issued.

Initialization

Initialization is a process whereby RB and KT token types can be programmed by BlackShield ID. This process applies the appropriate token template and inserts randomized encryption keys and seed values into the token and database. (Refer to Token Templates on page 81). Initialization should be used;

- To add “unprogrammed” tokens to inventory.
- To modify passcode strength and other operating parameters of factory programmed or unprogrammed tokens.
- To reprogram a token with new randomized encryption keys and seed values before reissuing.

For instructions on initialization refer to Initialize Tokens on page 102.

Create

The create function adds MP software and SMS/OTP tokens to inventory.
Import Tokens

Token records for factory initialized hardware tokens are imported into the server from the Import Tokens Group.

To import token records:

1. Use the browse button to locate the token record file (.btk extension).
2. Check the “Apply Server-side PIN Policy” to apply the current BlackShield ID PIN policy to all tokens on import (Server-side PIN Policy on page 86). The results of the import are displayed and the Token Availability group is updated.

This process will not import a token if its serial number already exists in the token database. This is to ensure that the token database record is not accidentally overwritten. To re-import a token, first remove the token and then import the file. The following graphic shows a re-import after a token (312146788) has been removed from the server.

Initialize Tokens

The Initialize function is used to add RB or KT series hardware tokens that are not factory initialized to the BlackShield ID database. This function is also used to apply a new token template to any RB or KT series token.
A token initializer is required for this operation and must be connected to a USB port on the management console.

![KT-1, KT-2/3 Series Token Initializer](image)

![RB Series Token Initializer](image)

![KT-4/5 Series Token Initializer](image)

Remote management consoles may not have the required drivers. These can be loaded during the initialization process or can be manually installed by copying the drivers from the C:\Program Files\CRYPTOCARD\BlackShield ID\USB Initializer folder (default location).

**Preparing the KT series token for Initialization**

Starting with the KT-x off, press and hold the button until the display shows “Init” (approximately 3-4 seconds). Release and press the button again. The display will show the prompt: **RDY 4 IR**. Insert the token in the initializer with the LCD display facing the front of the initializer. Click “Initialize” in the Token Mgt group. Note that the KT-x will remain in the RDY 4 IR state for approximately 15 seconds. The token cannot be initialized while in any other state. Initialization will complete in 7-10 seconds.

By default the New Token radio button is selected. If a token has been highlighted in the token availability list before invoking the initialize function, the Existing Token radio button will be selected and the serial number of the token will be displayed. Note that initialization will not proceed if the serial number of the token inserted in the initializer does not match the displayed serial number.
It is not necessary to close the Initialize Token between tokens. To initialize a series of tokens, simply ensure the token is in the proper state as instructed above and click the Initialize button.

![Initialize Token](image)

**Figure 38 – Initial KT Series Token**

**Preparing the RB series token for Initialization**

Place the RB-x token in the initializer with the LCD display down and facing the front of the initializer. The RB-x does not need any other preparation before initialization. Click “Initialize” in the Token Mgt group to complete the process. Initialization will complete in 7-10 seconds.

![Initialize Token](image)

**Figure 39 – Initialize RB Series**

By default the New Token radio button is selected. If a token has been highlighted in the token availability list before invoking the initialize function, the Existing Token radio button will be selected and the serial
number of the token will be displayed. Note that initialization will not proceed if the serial number of the token inserted in the initializer does not match the displayed serial number.

It is not necessary to close the Initialize Token between tokens. To initialize a series of tokens, simply ensure the token is in the proper state as instructed above and click the Initialize button.

Software tokens

Software tokens are added to the Token Availability list by clicking the Create button in the Token Mgt group. Software tokens can only be added if allowed by the BlackShield ID license installed on the system. The type of software token that is created is determined by the settings in the Token File Creation section of the Policy Tab (refer to Token File Creation on page 91). CRYPTOCard recommends using the MP token type.

Create

To create software tokens on the server, click the Create button, then select the type of token to be created, followed by Create. Click the Create button as often as necessary to create the desired quantity of tokens.

The SMS Token option will not appear unless the System Admin tab, SMS Settings section has been configured.

There is no limit to the number of software tokens that may be added to the Token Availability list; however, it is not possible to assign more tokens than permitted by the server license.

Note: The create process generates software tokens that conforms to the policy set in the current token template. There is no limit to the number of times a software token can be issued or revoke, created or
removed from the server. For security reasons the encryption key and seed values are randomized each
time, a token is reissued or created.

**MP Token**

Select the MP token option to create a token that can be loaded on computer hard drives, secure flash
drives, BlackBerry, Java enabled phone or iPhone. To restrict the type of device upon which the MP token
can be installed, refer to Token File Creation on page 91. With the exception of the BlackBerry and Java
phone, multiple MP tokens can be installed on a device, provided the UserID is unique for each token.

**SMS Token**

Select the SMS Token option to create a token that delivers passcodes via SMS message. This setting is
only available if the SMS section of the System Admin tab has been configured.

**Token Search**

The Token Search group functions are used to refine the Token
Availability list.

<table>
<thead>
<tr>
<th>Token Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>All</td>
<td>All tokens will be found by the search. This is the default value for this field.</td>
</tr>
<tr>
<td>KT</td>
<td>Refers to all KT type tokens registered in the server.</td>
</tr>
<tr>
<td>RB</td>
<td>Refers to all RB type tokens registered in the server.</td>
</tr>
<tr>
<td>MP</td>
<td>Refers to MP software tokens.</td>
</tr>
<tr>
<td>Legacy</td>
<td>Refers to older versions of software tokens. Generally these have been imported into BlackShield ID from older authentication server versions.</td>
</tr>
<tr>
<td>SMS</td>
<td>Refers to all SMS type tokens registered in the server.</td>
</tr>
<tr>
<td>OATH</td>
<td>Refers to all OATH type tokens registered in the server.</td>
</tr>
<tr>
<td>CUSTOM</td>
<td>Refers to all CUSTOM type tokens registered in the server, such as GrIDsure</td>
</tr>
</tbody>
</table>
Token State

Searches the token database for the selected token state where:

All

All tokens will be found by the search regardless of state. This is the default value for this field.

Inventory

Refers to any token that is registered in BlackShield ID but requires re-initialization before it can be issued to a user. This state will occur if the token was issued to a user and subsequently revoked as ‘Return to inventory initialization required’. Select the token and click Detail to view the token state and history.

Assigned

Refers to a token that has been assigned but cannot be used to authenticate. Normally the assigned state reflects a token that has been issued to a user via the self-enrollment function. Upon completion of self-enrollment, the state will change to active and the user can authenticate.

Active

Refers to a token that can be used to authenticate.

Suspended

Refers to a token that is assigned to a user but has been suspended and therefore cannot be used to authenticate. Suspension is the result of an Operator action to deal with events such as a forgotten token. An SMS token or a temporary static password (if enabled on the Policy Tab) can be assigned to a user with a Suspended token.

Locked

Refers to a token that cannot be used to authenticate because the account is locked. The state is returned to active when the account is unlocked or the Operator ‘Activates’ the token. A token becomes locked when the Authentication Threshold policy is exceeded. Refer to: Authentication Thresholds Group on page 85.

Lost/Failed

Is a state that can be assigned to a token by an Operator to reflect a lost, damaged or failed token. Tokens in this state remain in inventory until manually removed. Tokens may also be placed in the Lost state if the ‘Set assigned tokens to Lost’ threshold is exceeded (refer to: Self-enrollment group on page 71).

Initialized

Refers to a token that can be issued to a user.

Token Serial

Searches the token database for the specified serial number. Wild card searches are supported.

These fields may be combined in a single search. Click ‘Search’ to execute the search. Clear the search fields and click ‘Search’ to display all tokens in the Token Availability Group.
Token Management

These buttons are used to manage tokens. To use these buttons, select a token from the Token Availability Group then click one of the buttons.

Detail Button

This button is used to display operating parameters and usage statistics of tokens highlighted in the Token Availability list.

![Token Detail](image)

- **State**
  - **Initialized**: Token can be assigned to a user
  - **Not Initialized**: Token is in inventory but must be initialized before it can be assigned to a user.
  - **Enrolled**: Token has been assigned to the user via self-enrollment. The self-
enrollment process has not been completed.

<table>
<thead>
<tr>
<th>State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active</td>
<td>Token is active and can be used to authenticate</td>
</tr>
<tr>
<td>Manual Suspension</td>
<td>Token is assigned to user but has been manually suspended by an Operator. Token cannot be used to authenticate.</td>
</tr>
<tr>
<td>Lost Token</td>
<td>Token has been revoked and marked as lost.</td>
</tr>
<tr>
<td>Damaged Token</td>
<td>Token has been revoked and marked as faulty.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last State Change</td>
<td>Reflects the date and time of the most recent state change</td>
</tr>
<tr>
<td>Next PIN Change</td>
<td>Is the date for the next scheduled PIN change. This date is determined by settings on the Policy Tab.</td>
</tr>
<tr>
<td>In Service</td>
<td>Is a permanent record of the date and time that the token was first imported or initialized on the server. Subsequent initializations will not change this date, unless the token is first removed from the system and reimported or initialized.</td>
</tr>
<tr>
<td>Last Initialized</td>
<td>Is the date and time the token was last initialized.</td>
</tr>
<tr>
<td>Activated</td>
<td>Is the date and time the token was activated either by the Operator during manual assignment or reactivation or by the user when completing self-enrollment.</td>
</tr>
<tr>
<td>Last Auth. Date</td>
<td>Is the date and time the user last attempted to authenticate.</td>
</tr>
<tr>
<td>Result</td>
<td>Is the outcome of the user’s last attempt to authenticate: Success, Failure, Challenge, Server PIN Provided, User PIN Change Outer Window Authentication, Change Static Password, Password change Failed, PIN change Failed.</td>
</tr>
<tr>
<td>Total Auth</td>
<td>Is the total number of authentication attempts using this token.</td>
</tr>
<tr>
<td>Total OTP Pass</td>
<td>Is the total number of successful authentication attempts using this token.</td>
</tr>
<tr>
<td>Total OTP Fail</td>
<td>Is the total number of failed authentication attempts using this token.</td>
</tr>
<tr>
<td>Last Fail Date</td>
<td>Is the date and time of the last failed authentication using this token.</td>
</tr>
<tr>
<td>Is ICE Token</td>
<td>Has the token been flagged to be used as an In Case of Emergency (ICE) token. This option is only enabled if an ICE license has been installed.</td>
</tr>
<tr>
<td>Comment</td>
<td>Will show the last Operator comment attached to this token. Generally this field is blank unless the token has been suspended or revoked and a notation has been added by the Operator.</td>
</tr>
</tbody>
</table>
Initialize This button is used to reprogram RB and KT series tokens. Refer to: Initialize Tokens on page 102.

Remove This button is used to remove a token from the server.

Note: Removing a token from the server does not remove authentication and token history.

Create This button is used to add MP and SMS tokens to the server. Refer to Create on page 105.

Issuing Tokens

There are 4 ways to issue tokens to users:

- **Assign**: use this method to manually assign a token to a user. Tokens issued using this method are immediately active and can be used to authenticate.

- **Self-enroll**: use this method to manually issue tokens to many users. Tokens issued via this method cannot be used until the intended users have completed self-enrollment. This method is recommended for all token types, especially when the security of electronic or physical delivery of tokens cannot be assured. This method is also ideal where flexibility is required to seamlessly and transparently transition users from static passwords to token authentication over a period of time.

- **Use Rule-based provisioning** based on LDAP group membership available through the System Config tab: use this method to issue tokens automatically from LDAP based on group membership. As with the enroll function, tokens issued via this method cannot be used until the intended user has completed self-enrollment. This method is recommended for all token types and widely dispersed users populations. It is also ideal where flexibility is required to transparently transition users from static passwords to token authentication over a period of time. Refer to Rule-based Provisioning on page 120.

- **Use the Command Line Interface (CLI)**: This method provides a way to script assignment or enrollment functions and is ideal for use with 3rd party provisioning software. The CLI supports most of the token and user management functions available through the UI. Refer to Command Line Interface (CLI) Provisioning on page 123.

Assign Token Function

This function is used to issue a token that can be used immediately by the user for authentication. Generally this function is used if secure delivery of the token to the user can be assured. If a software token is to be delivered electronically or a hardware token will be delivered by a 3rd party such as a courier service, consider using Self-enrollment or rule-based provisioning instead.
Assign Hardware Tokens

To issue a hardware token using the Assign function:

1. Highlight the user to whom the token will be issued from the Users list.
2. Highlight the token to be issued to the user from the Token Availability list.
3. Click the Assign button.
4. Set access restrictions if required, then click Assign. Refer to Access Restrictions on page 118.

The token can now be used to authenticate. Note that the token state has been updated to “Active” in the Token Availability list. In addition the Assigned Tokens list in the highlighted User Detail has been updated.

Assign Software Tokens

Issuing software tokens via Assignment requires that two components be delivered to the end-user: the MP software application for the target device and the unique MP initialization file which personalizes the token for the user. The nature of the target device determines the options for delivery and installation of the MP software and initialization file.

Hard Drive Installation

The MP software can be installed on the target hard drive prior to assignment by:

Note: the initial PIN is displayed in the Token Availability list to assist Security Administrators during manual issuing of tokens. The PIN will be removed from the display on first PIN change. CRYPTOCard recommends that all tokens be issued with a changeable PIN and that change PIN on first use be enabled.

The user can now be viewed and managed from the Secured Users Tab.
- Manually installing the software.
- Pushing the software to the user machine using a 3rd party tool such as Microsoft SMS, Tivoli or Sun Identity Manager.

Once the software is installed the initialization file must be copied to the user’s hard drive where it can be imported into the software.

While it is possible to email the initialization file to the user enabling them to complete the hard drive installation process, this practice is not recommended by CRYPTOCard. If it is necessary to electronically deliver the initialization file to the user, CRYPTOCard recommends using the secure Self-enrollment process.

**BlackBerry Installation**

The MP software must be installed on the BlackBerry device prior to issuing the token via self-enrollment using either:

- BlackBerry Enterprise Server (BES).
- BlackBerry Desktop (USB) Manager.

The assignment process provides an option to “Issue” the MP for BlackBerry, which causes the initialization file to be sent by email to the user, preceded by a separate email which contains the initial PIN required to activate the token.

**IronKey Enterprise Secure Flash Driver Installation**

The MP software is pre-installed on all IronKey Enterprise products. The initialization file is delivered to the user during self-enrollment.

**SMS/OTP Zero footprint tokens**

SMS/OTP tokens can be issued to any user with a device capable of receiving an SMS message. The only requirement is that the User Detail includes the properly formatted phone number of the user’s mobile device.

Phone numbers must be in the format: ABC where:

- **A** – is the country code.
- **B** – is the city code.
- **C** – is the phone number.
Example 1: North American numbers would be in the format: 12128881111 where 1 is the country code, 212 is the city code and 8881111 is the local number.

Example 2: UK numbers would be in the format: 447815232134 where 44 is the country code, 7815 is the city code and 232134 is the local number.

An SMS/OTP token is active immediately upon assignment. The first message will contain an initial PIN and a passcode. The initial PIN must be changed to a value that conforms to the Server-side PIN policy and known only to the user during the first authentication.

The text that forms the SMS/OTP message can be modified. Refer to CLL Files on page 187.

**Example MP Software Token Assignment**

To issue an MP software token using the Assign function:

1. Ensure that the MP software is installed on the target device before proceeding. Refer to the MP Software Token User Guide for information for installation on hard drives, secure Flash drivers and BlackBerrys.

2. Highlight the user to whom the token will be issued from the Users list.

3. Highlight the token to be issued to the user from the Token Availability list.

4. Click the Assign button.

   ![Figure 44 – Token Availability](image)

5. Set access restrictions if required, then click Assign. Refer to Access Restrictions on page 118. The token is now assigned to the user.

   ![Figure 45 - Assigned Tokens](image)

6. Highlight the token in the Assigned Tokens list then click the “Issue” button.
7. Select BlackBerry to email the initialization file to the selected users BlackBerry.

Select BlackShield MP to save the initialization file. This file will need to be transferred to the users target device for import into the token software. The actual installation method will vary depending on the device and described in the MP software token user guide.

```
Figure 46 – Issue MP Token
```

The user can authenticate with the software token once the initialization file has been imported into the software on the target device. Note that the token state has been updated to “Active” in the Token Availability list. In addition, the Assigned Tokens list in the highlighted User Detail has been updated.

In addition, the user can now be viewed and managed from the Secured Users Tab.

**Temporary Passwords**

BlackShield ID supports the assignment of temporary static passwords to users. While the use of static passwords is not recommended, there are times when a temporary static password is useful:

- If a user forgets or loses their hardware token.
- In situations where the only user data source is the internal SQL database and it is necessary to enforce BlackShield ID authentication at a network access point (e.g. VPN) before all users have received or activated their tokens.

Temporary passwords cannot be assigned to accounts with Active Tokens. They can only be assigned to accounts with no assigned tokens or with a token in the Suspended state.

The temporary password function is available only if enabled on the Policy Admin tab. The options to manually create temporary passwords, force password change on first use and set limits on the lifetime of a password are also set in this area. Refer to Temporary Password Policy on page 88.
Note that CRYPTOCard recommends using SMS/OTP tokens instead of temporary static passwords because this enforces the use of one-time passwords and can be implemented without the need to distribute hardware or software tokens. The only requirement is that users must have a device capable of receiving an SMS message.

Note: that CRYPTOCard recommends using PreAuth rules instead of temporary static passwords if it is necessary to enforce BlackShield ID authentication at a network access point (e.g. VPN) before all users maintained in an LDAP user data source have received or activated their tokens. PreAuth offers several options to transition uses from static passwords to token authentication, including accepting the current LDAP password for a defined period of time or until the token is activated. Refer to PreAuthentication Rules on page 131.

**Temporary Password Assignment**

To assign a temporary password:

1. Highlight the user from the Users List to whom the temporary password will be assigned.
2. Click the Password button.
3. Enter a static password in the Temporary Password field.

![Temporary Password](image)

Click the Random button to have BlackShield ID generate a random, policy compliant temporary password or if allowed, manually create a temporary password.

If enabled the Security Administrator may set User Access Restrictions. Refer to Access Restrictions on page 119.

The Assigned Tokens group is updated when the temporary password is assigned. In addition, the user may now be managed from the Secured Users tab.

![Assigned Tokens](image)

**Figure 47 – Temporary Password**

**Figure 48 – Assigned Tokens**
Self-Enroll Function

Self-enroll is a provisioning process that substantially reduces the time required to issue tokens to users and provides:

- secure electronic delivery of software tokens.
- secure physical delivery of hardware tokens via 3rd party.

In self-enroll, the Security Administrator assigns a token to the user but unlike the Assign function, the token cannot be used until it is enrolled by the intended recipient. The process is secure because only the intended user has the necessary information to complete the process which binds the token to the user and activates it for authentication.

The BlackShield ID generated user self-enrollment notification and instructions will vary depending on the type of hardware or software token being issued and the PIN policy. Notifications and instructions can be modified, including the addition of logos and other graphics.

To configure Allowed Target types and custom Self Enrollment dialogs, refer to the Allowed Targets Settings (Settings) section on page 91.

Self-enroll hardware tokens

To provision a user with a hardware token using self-enrollment:

1. Highlight the user to whom the token will be issued from the Users list.
2. Highlight the token to be issued to the user from the Token Availability list.
3. Click the Self-Enroll button.
4. Set access restrictions if required, then click Enroll. Refer to Access Restrictions on page 118.

BlackShield ID assigns the token and sends an email notification to the user which contains enrollment instructions, a unique URL and an activation code. The user must complete the enrollment within the Reservation Time to Live period (refer to: Self-enrollment group on page 71).

Self-enroll MP software tokens

As with assignment, issuing software tokens via self-enrollment requires that two components be delivered to the end-user: the MP software application for the target device and the unique MP
initialization file which personalizes the token for the user. The nature of the target device determines the options for delivery and installation of the MP software and initialization file.

**Hard Drive Installation**

The MP software can be installed on the target hard drive prior to assignment by:

- Manually installing the software.
- Pushing the software to the user machine using a 3\textsuperscript{rd} party tool such as Microsoft SMS, Tivoli or Sun Identity Manager.

Alternatively, if during self-enrollment the MP software is not detected on the target hard drive, the user will automatically be presented with links to the MP software installers and prompted to install the software.

The self-enrollment process continues when the MP software is detected, automatically loading the initialization file, prompting the user to create or change a PIN according to PIN policy.

**Note:** Please ensure the 64-bit version of Internet Explorer is used during enrollment on 64-bit operating system.

**IronKey Enterprise Secure Flash Driver Installation**

The MP software is pre-installed on all IronKey Enterprise products. The initialization file can be delivered via Self-Enrollment.

**Example MP Software Token Self-Enrollment**

To provision a user with an MP software token using Self-enrollment:

1. Highlight the user to whom the token will be issued from the Users list.
2. Highlight the token to be issued to the user from the Token Availability list.
3. Click the Self-Enroll button.
4. Set access restrictions if required, then click Enroll. Refer to Access Restrictions on page 119.

BlackShield ID assigns the token and sends an email notification to the user which contains enrollment instructions, a unique URL and an activation code. The user must complete the enrollment within the Reservation Time to Live period (refer to: Self-enrollment group on page 71)

The user can authenticate with the software token on completion of Self-enrollment. Note that the token state has been updated to “Active” in the Token Availability list. In addition, the Assigned Tokens list in the highlighted User Detail has been updated.

The user can now be viewed and managed from the Secured Users Tab.

Access Restrictions

The Access Restrictions dialogue is used to limit the time, day and date ranges on which a user can authenticate. This dialogue is disabled if “Allow User Restrictions” is disabled on the Policy Tab. Refer to Restrictions Group.

Though Access Restrictions can be placed on any account, this function is normally only applied to users accounts in the internal SQL user data source. CRYPTOCard recommends applying PreAuth rules for users held in an LDAP user data source so that changes to LDAP attributes, such as time/day access restrictions, group membership and account status are automatically enforced by BlackShield ID.
Figure 49 - Assign Token / Access Restrictions

Enable Access Restrictions  Check this box to apply access restrictions to the user account.
Start Date  The user will not be able to authenticate before this date.
End Date  The user will not be able to authenticate after this date.
Start Time  The user will not be able to authenticate before this time.
End Time  The user will not be able to authenticate after this time.
Day of the week  The user will only be able to authenticate on “checked” days of the week.
Rule-based Provisioning

Rule-based provisioning of tokens based on LDAP group membership is one of the most powerful workflow automation facilities of BlackShield ID. Essentially this facility is used to be automatically issued or revoke tokens based on LDAP group membership.

Rule-based provisioning emulates the functionality of the self-enroll button on the Assignment Tab. Recall that this button causes a token to be assigned to the user, who upon receipt, can activate the token by completing the self-enrollment process. By creating rules based on LDAP membership, the need for the Security Administrator to issue the token through the management console is eliminated.

To enable rule-based provisioning, BlackShield ID must be configured to monitor one or more groups for changes in membership. Upon detecting a change, one of the following actions will occur:

- If a user is added to the group, BlackShield ID will auto provision the user with the specified token type. Depending upon the token type and security policy, the user may be required to complete self-enrollment to activate the token and change the initial PIN. Note that SMS tokens are immediately active and do not require self-enrollment, however, if the server-side PIN policy requires a PIN change, the user must complete this step during the first authentication.
- If the user is removed from the group and auto revoke is enabled, the token will automatically be revoked.

Rule-based provisioning can be used in conjunction with PreAuth rules to further control or restrict access to protected resources, or to prevent authentication if the account is locked or suspended in LDAP.

Configure Rule-based Provisioning

Auto provision is configured from the System Admin tab.

1. Create the LDAP group to be monitored by BlackShield ID. Example: SMS-ICE.

2. Click the Configure button in the Provisioning Rules Setting group on the System Admin Tab.

   ![Provisioning Rules Settings](image)

   **Figure 50 - Provisioning Rules Settings**

3. Click Add to create a new rule, Remove to delete an existing rule or View to view an existing rule.
4. Assign a Rule Name.

5. Select the type of token to be provisioned from the dropdown.

6. Select the group(s) to be monitored from the Groups list and add them to the monitored groups list.

7. Click Done to save the rule.

8. The provisioning delay setting determines the frequency with which BlackShield ID checks the monitored groups for changes. Adjust the default value as required then click the Apply button in the Actions group to save the change.

In the example above, a SMS/OTP token will be issued to any member of the SMS LDAP group within 5 minutes of becoming a member. Likewise, the SMS/OTP token will be revoked within 5 minutes of their removal from the group.
Command Line Interface (CLI) Provisioning

The CLI provides an alternative to the management console GUI for a range of user and token functions including the issuance of tokens. The CLI can be used to:

- Create, modify or delete user accounts and groups in the internal SQL user data source.
- Create and add software tokens to the database.
- Modify tokens including force PIN changes and reinitialize.
- Invoke the Self-enrollment process.

Command Line Interface Syntax

Connect

Syntax: Connect server[:port] User_Name [-p] OTP [-s]

Example: Connect 192.168.232.163 jbrown 32416273 -s

Usage: This command is required to create a connection between the CLI and the BlackShield ID server after which other commands may be applied.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>server[:port]</td>
<td>Hostname or IP of the BlackShield ID server with optional port</td>
</tr>
<tr>
<td>USER_NAME</td>
<td>UserID of an Operator configured on the BlackShield ID server</td>
</tr>
<tr>
<td>-p</td>
<td>Prompts for a no echo OTP</td>
</tr>
<tr>
<td>OTP</td>
<td>OTP or static password to authenticate the User_Name account. Not required with –p switch.</td>
</tr>
<tr>
<td>-s</td>
<td>Connect using HTTPS</td>
</tr>
</tbody>
</table>
New

Syntax:    New Object_Type

Example:    New user jbrown j-m

Example:    New token –authversion V7

Usage:  Use this command to create users, software tokens and containers in the internal SQL user data source.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Object_Type</td>
<td>Object to add to the database. Can be one of the following:</td>
</tr>
<tr>
<td>Container</td>
<td>Name of the container to add to the database.</td>
</tr>
<tr>
<td>User</td>
<td>Indicates that a UserID is to be created.</td>
</tr>
<tr>
<td>USER_NAME</td>
<td>Name of user to add to the database in the specified container.</td>
</tr>
<tr>
<td>[container_name]</td>
<td>Name of the container in which the user should be created.</td>
</tr>
<tr>
<td>Token</td>
<td>Indicates that a token is to be created.</td>
</tr>
<tr>
<td>[-subtype ST</td>
<td>UB</td>
</tr>
</tbody>
</table>

Initialize

Syntax:    Initialize TOKEN_SERIAL [-isLocal true|false]

Example:    Intialize 760001212 –isLocal false

Usage:  Changes the state of an assigned software token to Active and generates an initial PIN. This is the equivalent of the console “Issue” function.
Parameters | Description
---|---
TOKEN_SERIAL | Serial number of token assigned to a user
[-isLocal true|false] | Location to which initialization file will be saved. False = Default file location set on Policy Admin Tab.

**Update**

Syntax: 

Example: 
update user jbrown -unlock -restrictions true -days 0111110

Usage: When applied to a user; this function updates a static password, access restrictions or unlocks a user account. When applied to a token; this function assigns/unassigns, activates and/or sets a PIN.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Object_Type</strong></td>
<td></td>
</tr>
<tr>
<td>User</td>
<td>Update a user as follows:</td>
</tr>
<tr>
<td>USER_NAME</td>
<td>Name of the UserID that will be updated.</td>
</tr>
<tr>
<td>[-password]</td>
<td>Assigns a static password to the User which must be used to authenticate against BlackShield ID. Password must confirm to password policy. Do not specify a password to remove an assigned password.</td>
</tr>
<tr>
<td>[-unlock]</td>
<td>Unlocks a user account.</td>
</tr>
<tr>
<td>[-restrictions true</td>
<td>false]</td>
</tr>
<tr>
<td>[-days #######]</td>
<td>Each # represents a day of the week, commencing with Sunday. User can authenticate on allowed days. 1 = allowed, 0 = denied.</td>
</tr>
<tr>
<td>[-startTime HH:MM:SS]</td>
<td>HH:MM:SS represents the earliest time of day the user can authenticate. Where HH = 00 to 23, MM = 00 to 59, SS = 00 to 59.</td>
</tr>
<tr>
<td>[-endTime HH:MM:SS]</td>
<td>HH:MM:SS represents the latest time of day the user can authenticate. Where HH = 00 to 23, MM = 00 to 59, SS = 00 to 59.</td>
</tr>
</tbody>
</table>
[-startDate YYYYMMDD]  YYYYMMDDD represents the first date the user can authenticate. Where YYYY= year in digits, MM = 01 to 12, DD = 01 to 31.

[-endDate YYYYMMDD]  YYYYMMDDD represents the last date after which the user cannot authenticate. Where YYYY= year in digits, MM = 01 to 12, DD = 01 to 31.

Token

TOKEN_SERIAL  This is the serial number of the token to be updated.

[-owner]  Assigns and activates token to the specified UserID. Use this switch without specifying a UserID to de-assign the token.

[-enable]  Reactivates a suspended token.

[-pin]  Sets a PIN for the token. PIN must comply with PIN Policy.

Enroll

Syntax:    enroll USER_NAME [serial] [-type MP|KT|RB]

Example:    enroll jbrown –type MP

Usage: The enroll command is used to initiate self-enrollment provisioning for MP, KT and RB token types. This is equivalent to the console “Self-enroll” function.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>USER_NAME</td>
<td>User ID to whom a token will be provisioned using self-enrollment..</td>
</tr>
<tr>
<td>[-serial]</td>
<td>Specifies the serial number of the token to be assigned to the UserID.</td>
</tr>
<tr>
<td>[-type MP</td>
<td>KT</td>
</tr>
</tbody>
</table>

Moveuser

Syntax:    moveuser USER_NAME Container

Example:    moveuser jbrown j-m
Usage: use this command to move a user to a different container in the internal SQL user data source.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Object_Type</td>
<td></td>
</tr>
<tr>
<td>User_Name</td>
<td>User ID to whom a token will be provisioned using self-enrollment</td>
</tr>
<tr>
<td>Container</td>
<td>Name of the container to which the user will be moved.</td>
</tr>
</tbody>
</table>

List

Syntax: List Object_Type

Example: List User

Usage: lists users or containers

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Object_Type</td>
<td></td>
</tr>
<tr>
<td>Container</td>
<td>User ID to whom a token will be provisioned using self-enrollment</td>
</tr>
<tr>
<td>User</td>
<td>Name of the container to which the user will be moved.</td>
</tr>
</tbody>
</table>

Cd

Syntax: cd \SQL

Usage: change to a different container

Delete

Syntax: Delete Object_Type

Example: Delete user jbrown

Usage: use this command to remove users, containers from the internal sql user data source or to remove tokens from the server.
<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Object_Type</td>
<td></td>
</tr>
<tr>
<td>User</td>
<td>Update a user as follows:</td>
</tr>
<tr>
<td>USER_NAME</td>
<td>Name of the UserID that will be removed.</td>
</tr>
<tr>
<td>Token</td>
<td></td>
</tr>
<tr>
<td>TOKEN_SERIAL</td>
<td>This is the serial number of the token to be removed.</td>
</tr>
<tr>
<td>Container</td>
<td></td>
</tr>
<tr>
<td>CONTAINER_NAME</td>
<td>This is the container name to be removed</td>
</tr>
</tbody>
</table>

**Help**

Syntax: `Help`

Usage: generates context sensitive help.

**Quit**

Syntax: `Quit`

Usage: disconnects and closes the command line client.
Revoking Tokens

Tokens can be revoked using the console, rule-based provisioning or the command line interface.

Revoke using the console

Tokens can be revoked from the Assignment or Secured Users tab.

![Figure 52 - Revoke from Assignment Tab](image)

![Figure 53 - Revoke from Secured Users Tab](image)

In both cases the Security Administrator must:

- Select the user to whom the token is currently assigned.
- Highlight the token to be revoked.
- Click the revoke button.
- Select a revocation option.
- Click Revoke to confirm the action.

Revoke Options

BlackShield ID presents several revocation options as shown in Figure 54 - Revocation Options.
A revoked token can no longer be used to authenticate. If the "Revoke Password" option is not selected the user can still authenticate using the assigned temporary password.

**Figure 54 - Revocation Options**

**Return to Inventory, initialization required**
This option returns the token to inventory, however the token cannot be re-issued until it is re-initialized. This option is normally selected for hardware tokens that have been initialized with token-side changeable PINs because only the current user will know the PIN value required to enable the token. Re-initialization provides the opportunity to reset the PIN to a new value, change the type of PIN used and to regenerated keys, seeds and other operating parameters.

**Return to Inventory**
This option returns the token to inventory from which it can be reissued. This option is normally selected for all software and hardware tokens configured for Server-side PINs. Note that all software tokens reissued by BlackShield ID use new, randomly generated keys and seed values. This security feature allows software tokens to be reissued as often as required without the need to recover the token from the previous user.

**Lost**
This option marks the revoked token as lost, making it unavailable for reissue. A token in the lost state can be reintroduced to inventory through initialization or re-import.
Fault         This option marks the token is faulty, making it unavailable for reissue. A token in the lost state can be reintroduced to inventory through initialization or re-import.

Comment      This is a free-form comment area in which the Security Administrator can add a comment regarding the revoke action. This forms a permanent part of the token history record.

Revoke Password This option is available if the user has a static password for authentication against BlackShield ID. In most cases a temporary static password will have been assigned when a token is Suspended. Refer to Suspend Button on page 146.

Rule-based Revocation

Tokens are automatically revoked when a user is removed from one of the monitored LDAP groups. Refer to Rule-based Provisioning on page 121.

Command Line Revocation

Tokens can be revoked using the Update command. Refer to Update on page 125.
Chapter 9 – Advanced Authentication

Just because a user is able to provide a valid one-time passcode does not necessarily mean that they should be granted access to the network. Other conditions such as network access point, group membership, account status and other attributes might be important in allowing or denying access.

Security Administrators can use PreAuthentication Rules to apply additional conditions that must be met for authentication to succeed.

The key advantages of PreAuthentication Rules are:

- Rules can be applied to LDAP user account attributes
- Rules can be applied to user accounts maintained in the internal SQL user data source
- Rules can be applied based on network access points (source IP, Agent)
- Rules can be used to modify the authentication sequence (OTP, LDAP, LDAP + OTP)
- Changes to user attributes made in LDAP or the internal user data source are immediately effective on BlackShield ID

PreAuthentication Rules

There are few limitations to how PreAuthentication Rules can be used. Rules can be relatively simple, checking a single attribute such as time of day restrictions or can check multiple attributes such as group membership, network access point and token state.

The authentication proceeds in the following sequence:

4. UserID is validated. If valid:
5. Pre-authentication rules are applied. If any rule is satisfied:
6. Password is validated. If valid access is granted.

The key concepts to consider when creating rules are:

- Multiple rules may be configured, however a user’s attributes need only satisfy one rule for authentication to proceed.
- Initially BlackShield ID is configured with an “Allow All” rule. Pre-Authentication Rules must be enabled to provide the restrictions.
Authentication Attributes

The following is a list of the attributes that can be incorporated into rules:

Agent is

This attribute is used to specify which agents are allowed to connect with the server. For example, Agent is IAS would allow RADIUS authentication from all Microsoft IAS/NPS servers with the appropriately configured BlackShield IAS/NPS agent.

<table>
<thead>
<tr>
<th>Attribute / Filter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agent is</td>
<td></td>
</tr>
<tr>
<td>Authentication API</td>
<td>Required to allow authentication from 3rd party applications that added authentication using the BlackShield ID Authentication API.</td>
</tr>
<tr>
<td>Citrix</td>
<td>Required to allow authentication via the BlackShield ID Agent for Citrix Web Interface.</td>
</tr>
<tr>
<td>Console</td>
<td>Required to allow remote management connections to BlackShield ID server</td>
</tr>
<tr>
<td>IAS</td>
<td>Required to allow authentication via the BlackShield ID Agent for IAS / NPS</td>
</tr>
<tr>
<td>IIS</td>
<td>Required to allow authentication via the BlackShield ID Agent for IIS</td>
</tr>
<tr>
<td>Remote Management API</td>
<td>Required to allow the Command Line Interface (CLI) to connect to BlackShield ID server.</td>
</tr>
<tr>
<td>Juniper / Funk SBR</td>
<td>Required to allow authentication via the BlackShield ID Agent for Juniper/Funk Steel Belted RADIUS</td>
</tr>
<tr>
<td>Windows Logon</td>
<td>Required to allow authentication via the BlackShield ID Agent for Windows Domain Logon.</td>
</tr>
</tbody>
</table>
**Date Restrictions**

This attribute is used to limit the lifetime of a rule. This rule is always used in conjunction with another attribute. For example, it could be used with the “LDAP password pass through” attribute to facilitate migration from LDAP passwords to token authentication, whereby LDAP passwords would be valid against BlackShield ID until the rule expires or a token is activated.

<table>
<thead>
<tr>
<th>Attribute / Filter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date Restrictions</td>
<td></td>
</tr>
<tr>
<td>Begin this rule on</td>
<td>If enabled, the rule will not be active until the indicated date. If disabled, the rule is immediately effective.</td>
</tr>
<tr>
<td>Expire this rule on</td>
<td>If enabled, the rule will stop being enforced on this date. If disabled, the rule will remain active.</td>
</tr>
</tbody>
</table>

**IP**

If enabled, BlackShield ID will not process authentication requests from NAS devices such as VPNs and firewalls that have an IP address outside of the defined range. This attribute is usually used in conjunction with another attribute. For example, if combined with a group membership attribute, only members of a specific group could authenticate at a NAS device in the IP range. Conversely, in the absence of any other contravening rule, members of the group would not be able to authenticate at NAS device not in the IP range.

<table>
<thead>
<tr>
<th>Attribute / Filter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP</td>
<td></td>
</tr>
<tr>
<td>Is equal to</td>
<td>Specifies a single valid IP address</td>
</tr>
<tr>
<td>Is in the range</td>
<td>Specifies an IP address range</td>
</tr>
<tr>
<td>Is in mask</td>
<td>Specifies an IP address range using a mask</td>
</tr>
</tbody>
</table>
**IP V6**

This attribute is identical in function to the IP attribute but provides support for IP V6 based networks.

<table>
<thead>
<tr>
<th>Attribute / Filter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP V6</td>
<td></td>
</tr>
<tr>
<td>Is equal to</td>
<td>Specifies a single valid IP address</td>
</tr>
<tr>
<td>Is in the range</td>
<td>Specifies an IP address range</td>
</tr>
<tr>
<td>Is in mask</td>
<td>Specifies an IP address range using a mask</td>
</tr>
</tbody>
</table>

**LDAP Password Pass Through**

This attribute determines when BlackShield ID should validate a password or pass it through to LDAP for validation. It also determines how BlackShield ID will handle LDAP authentications that fail.

The primary purpose of this attribute is transparent migration of users from static passwords to token authentication. For users that meet the conditions, authentication will “pass through” BlackShield ID to LDAP for validation. There is no need to create, manage or import the LDAP static password into BlackShield ID. It also determines the action to be taken by BlackShield ID after LDAP authentication. This attribute is usually combined with Date Restrictions and Agent or IP attributes.

For example, enabling LDAP Password Pass Through if a user has no token or temporary password would mean that any user with a token must use it to authenticate while those without could continue to use their LDAP password until they received or enrolled their token or until the Date restriction disabled this attribute.

<table>
<thead>
<tr>
<th>Attribute / Filter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LDAP Password Pass Through</td>
<td></td>
</tr>
<tr>
<td>Always</td>
<td>All passwords will be passed to LDAP for validation</td>
</tr>
<tr>
<td>When user has no BlackShield Token/Password</td>
<td>Passwords will be passed to LDAP for validation only if the user does not have a token in the Active, Suspended or Locked state.</td>
</tr>
<tr>
<td>If LDAP Authentication fails</td>
<td></td>
</tr>
<tr>
<td>Reject the authentication</td>
<td>Access is denied if LDAP authentication fails</td>
</tr>
<tr>
<td>Forward request to BlackShield</td>
<td>BlackShield attempts to validate the password.</td>
</tr>
</tbody>
</table>
User is a member of

This attribute is used to require group membership for authentication to proceed. It is normally used in conjunction with Agent or IP attributes so that a user must be a member of a specified LDAP group when authenticating at the defined agent or IP address.

This attribute does not require group membership to be configured in BlackShield ID. Instead, the users LDAP group memberships are checked with each authentication. This means that group membership is managed from LDAP.

<table>
<thead>
<tr>
<th>Attribute / Filter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User is a member of</td>
<td>User must be a member of the specified group in the list. To create a list, separate LDAP group names with a semi-colon “,”</td>
</tr>
</tbody>
</table>

User is in container

This attribute is the equivalent of “User is a Member of” but applies only to users organized in containers (refer to Containers Tab on page 138) in the internal SQL user data source. Used. It is normally used in conjunction with Agent or IP attributes so that a user must be a member of a specified container or one of its sub containers when authenticating at the defined agent or IP address.

<table>
<thead>
<tr>
<th>Attribute / Filter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User is in container</td>
<td>To create a list, separate containers with a semi-colon. “,”</td>
</tr>
<tr>
<td>Only</td>
<td>User must be a member of the specified container in the list.</td>
</tr>
<tr>
<td>Or one of its sub containers</td>
<td>User must be a member of the specified container in the list or one of its sub containers</td>
</tr>
</tbody>
</table>
Configuring Pre-Authentication Rules

To configure rules, click Configure in the Pre-Authentication Rules group on the System Admin tab.

![Pre-Authentication Rules](image)

**Figure 55 - Pre-Authentication Group**

By default Pre-Authentication Rules are disabled, this allows all BlackShield agent authentication requests to the BlackShield server (Allow All). When Enable Pre-Authentication Rules is selected, all BlackShield agent traffic is denied (Deny All). You must select specific rules for incoming BlackShield agent authentication requests.

Click Add to create a new rule and open the Add Rule dialogue.

Highlight a rule and click edit to modify an existing rule.

Highlight a rule and click Remove to delete the rule.

Click System Rule to review all rules.

To add a rule, select a filter from the dropdown list then add or select options. Repeat the process to add multiple attribute filters to the rule.

To remove an attribute filter, highlight it then click remove.

Click Done to complete and save the rule.

![Add Rule](image)

**Figure 57 - Adding a Pre-Authentication Rule**
Authentication Activity Pane

If a Pre-authentication rule prevents an authentication from proceeding, a message to this effect will be displayed as the cause of the failure. This identifies users attempting to access a resource protected by a rule.

<table>
<thead>
<tr>
<th>TimeStamp</th>
<th>Host</th>
<th>Action</th>
<th>Result</th>
<th>Serial</th>
<th>IP</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/22/2009 12:53:26 AM</td>
<td>192.168.1.1</td>
<td>Authentication</td>
<td>Failure</td>
<td>127.0.0.1</td>
<td></td>
<td>Denied by Pre-Auth Rule</td>
</tr>
</tbody>
</table>

Figure 58 - Authentication Denied - Pre-Auth Rule
Chapter 10 – Internal SQL User Source Containers

Containers Tab

The internal SQL user data source can be subdivided into containers, into which users can be created or moved. Containers serve three purposes:

- They provide a way to organize users into groups for management convenience
- If using the Juniper Belted RADIUS agent, BlackShield ID can return the container path for use as a RADIUS Group return attribute which in turn can be used by the RADIUS client (firewall, VPN, etc.) to enforce access restrictions.
- Pre-Authentication rules can be applied to users based on their container attribute.

![Figure 59 – Containers Tab](image)

The containers tab is separated into two panes: the Containers Group and the Users group.
Containers Group

The Containers Group displays an expandable list of all containers found in the LDAP and internal SQL user data sources. LDAP containers cannot be modified as BlackShield ID does not write or modify LDAP. They are displayed as an aid to creating Pre-Authentication rules based on LDAP containers.

Containers can be added to the SQL hierarchy by highlighting the container under which the new container should be created.

**Container Detail:** This is the current Path. The list of users displayed in the Users group corresponds to this path.

**Add:** This Button adds a Container to the internal SQL user data source. The new container will be added below the currently selected container.

**Remove:** This button removes a Container and any users it contains from the internal SQL user data source.

This function must be used with care since Sub Containers and all users they contain will be deleted from the system by this action.

**Move:** This Button is used to change the location of a container in the hierarchy. All sub containers and all users residing in those containers will be moved. To move a container, click Move, expand the containers list, and then highlight a container in the list under which the container should be moved. Click OK to complete the process.
Users Group

This group provides the ability to Search for and Move users between Containers. The Search function may be used to find a User or group of users within a Container. Once located, the User or group of users may be moved to another container.

Search: enter search criteria into any combination of search fields then click Search to refine the list of users. The * symbol can be used as a wild card following the last character in any field.

Move: place a check beside all users to be moved, and then click the Move button.

Expand the containers list and highlight the destination container, then click OK.
Chapter 11 - Help Desk

Users that can authenticate against BlackShield ID can be managed from the Secured Users tab which provides user and token management functions that are typical for help desks.

Secured Uses Tab

The Secured User Tab groups functions that relate to managing Secured Users, their tokens, and passwords. A number of functions are common with the Assignments Tab, however there are a number of key differences:

- Only users that have been assigned a token or temporary password from the Assignment tab are visible on this tab.
- It is not possible to assign a token to a user from this tab.
- It is not possible to modify or delete users maintained in the internal SQL user data source from this tab.
- It is not possible to modify Access Restrictions from this tab.
Secured User Search Group

This group provides the ability to search for users and tokens using a variety of criteria. The search function supports "*" wildcards and minimum matching. For example: bro, bro*n will find Brown and Browne while bro*ne will not find Brown. This search function will find all users and tokens in the specified containers.

User Search

- Last Name searches the ‘Last Name’ field.
- First Name searches the ‘First Name’ field.
- User ID searches the ‘User ID’ field.
- These fields may be combined in a single search. Click ‘Search’ to execute the search. Clear the search fields and click ‘Search’ to display all users in the Users Group.
The results of the search are displayed in the Secured Users List.

Token Search

Token Serial number searches the token database for the specified serial number. Wild card searches are supported. Only tokens that are Assigned or Active will be found with this search, displaying the User associated with the token displayed in the Secured User list.

Secured Users Group

This list displays all users or the result of the User search. The list can be sorted by clicking on any of the column headings. The sort toggles between ascending and descending sorts.

Clicking on a user will highlight the user and populate the User Detail Group, the Token Information, Access Restrictions, and the Authentication Metrics.
User Detail Group

The user detail group displays information about individual users highlighted in the Users List. This group also displays the Container information of the user selected. This information may be used to find the user on the Assignments Tab.

Token Information Group

The Token Information group displays information about all tokens and temporary passwords assigned to the selected user.
Access Restrictions Group

The Access Restrictions group displays information about restrictions that were applied to the account during token assignment.

Authentication Metrics Group

The Authentication Metrics group displays the number of successful and unsuccessful authentication attempts that have been made by the user. These metrics are the cumulative statistics for all tokens and temporary password authentications performed by the user.

Authentication Activity Group

This list displays the details on all Authentication attempts by the selected user. These are displayed by: Timestamp, Action, Result, Serial Number, IP and Agent. All columns may be sorted in ascending or descending order by clicking on the column heading.

Token Management Group

The Token Management Group provides token management functions including Suspending, Activating, Initializing, Revoking, Resyncing and Issuing Tokens as well as viewing token Details, or generating a New PIN. These buttons are only active if a token has been selected and the token is in the proper state as detailed below.
Details Button

The Details Button is available for all token states.

Highlight a token in the Token Information list. Click the Detail button to open the token detail dialogue. The dialogue displays the token operating characteristics that were applied during initialization or import. Refer to Token Management on page 107 for an explanation of this dialogue shown in Figure 64 - Token Detail on page 146.

Suspend Button

The Suspend Button is available for Active and Assigned token states and is used to suspend a token, preventing it from being used to authenticate.

Click the Suspend button to open the token Suspend dialogue. The features of this dialogue are enabled or disabled by the Temporary Password Policy. (Refer to: Temporary Password Policy on page 88).
Suspend Token

Suspending a token will prevent the user from authenticating. A temporary static password may be set if permitted by the security policy.

Temporary Password Assignment

- **Set temporary password**
- **Random**
- **Change password on first use required**

**Comment Field**

This section of the dialogue allows the Security Administrator to enter a free-form comment related to this action. This forms a permanent part of the token history and will be displayed in the Token detail dialogue.

**Clear**

The Clear Button allows the administrator to remove any information or selections made and return the dialogue to the original state.

**Suspend**

The Suspend Button activates the command, suspends the Users token and enables the Temporary Password if set.

---

**Figure 65 - Suspend Token**

Temporary Password Assignment

- Enter a temporary password that conforms to the temporary password policy or use the Random button to have the server generate a temporary password.

Set Temporary Password

- If this tick box is selected a password must be provided before the token can be suspended. If the tick box is cleared no temporary password will be assigned to the user and this section will no longer apply. Enter a temporary password that conforms to the temporary password policy or use the Random button to have the server generate a temporary password.

Change Password on First Use Required

- If this field is ticked the User must change the password set in this dialogue to one that only they know during their first logon.

Comment Field

- This section of the dialogue allows the Security Administrator to enter a free-form comment related to this action. This forms a permanent part of the token history and will be displayed in the Token detail dialogue.

Clear

- The Clear Button allows the administrator to remove any information or selections made and return the dialogue to the original state.

Suspend

- The Suspend Button activates the command, suspends the Users token and enables the Temporary Password if set.
Close

The Close button ends the dialogue and returns control to the Secured User Tab.

Results

This section of the dialogue provides the results of the Suspension action and will list the success or failure of the suspension and the assignment of the temporary password.

Unlock Button

The Unlock Button is used to activate a highlighted token that is in the suspended token or Locked state.

Click the Unlock button to open the Activate Token dialogue. The features of this dialogue are enabled or disabled by the Server-side PIN Policy and only if the token was issued with a Server-side PIN. (Refer to: Server-side PIN Policy on page 86).

**Figure 66 - Activate Token**

**Activation Options**

- **Set new PIN**
  - Enter PIN that conforms to the Server-side PIN policy or use the Random button to have the server generate a PIN.
- **Set new PIN Option**
  - If checked, a new PIN must be set. If cleared, the PIN in effect at the time the token was suspended is valid.
Change PIN on first use required. If checked, the user must change the PIN set or allowed in this dialogue during the next authentication.

Comment Field This section of the dialogue allows the Security Administrator to enter a free-form comment related to this action. This forms a permanent part of the token history and will be displayed in the Token detail dialogue.

Clear The Clear Button allows the administrator to remove any information or selections made and return the dialogue to the original state.

Activate The Activate Button completes this action and activates the token.

Close The Close button ends the dialogue and returns control to the Secured User Tab.

Results This section of the dialogue provides the results of the Activation action.

If a user has been assigned an RB or MP token and an Active state is detected, the remote unlock code dialog will appear. The locked RB or MP token will display Token Challenge code, which needs to be entered into the Token Challenge field. The BlackShield server will generate a Server Response code that can be manually entered into the RB or MP token to remotely unlock it allowing the user to generate one-time passwords.

Revoke Button

The Revoke Button is available for all token states and is used to revoke the token from the user and return it to Inventory.
Revoke Token

A revoked token can no longer be used to authenticate. If the ‘Revoke Password’ option is not selected the user can still authenticate using the assigned temporary password.

Return to Inventory, initialization required

If this is selected the token is returned to inventory but must be initialized again before it can be assigned to another user. Reinitializing the token will apply the corresponding token template, including new encryption keys and seed values.

Return to inventory

If this is selected, the token is returned to inventory and can be immediately reassigned to another user.

Lost

If this is selected the state is set to Lost/Failed. The token is returned to the Assignments Tab token list where it can be removed from the system or returned to inventory if it is found.

Faulty

This setting is similar to Lost. The token is returned to the Assignments Tab token list where it can be removed from the system or returned to inventory if it is functional.

Figure 67 - Revoke Token Dialogue

The window displays the serial number of the token selected and allows the administrator to choose the reason the token is being revoked.
Clear  The Clear Button allows the administrator to remove any information or selections made and return the dialogue to the original state.

Revoke  The Revoke Button activates the command and revokes the token. If the user has a temporary password, the password may remain after the token is revoked if the Revoke Password tick box is cleared. If this box is selected (default) the token and password will be removed. This box will be inactive if Policy Tab settings forbid a temporary password.

Comment Field  This section of the dialogue allows the Security Administrator to enter a free-form comment related to this action. This forms a permanent part of the token history and will be displayed in the Token detail dialogue.

Close  The Close button ends the dialogue and returns control to the Secured User Tab.

Results  This section of the dialogue provides the results of the Activation action.

**New PIN Button**

The New PIN Button is available for tokens in an Active state issued with a Server-side PIN. The features of this dialogue are enabled or disabled by the Server-side PIN Policy and only if the token was issued with a Server-side PIN. (Refer to: Server-side PIN Policy on page 86).

Highlight a token and click the New PIN button to open the New PIN dialogue.
Figure 68 - New PIN Mode Dialogue

Set PIN  
If this option is checked, enter a PIN that conforms to the PIN policy or use the Random button to have the server generate a PIN. If this option is unchecked a new PIN cannot be set.

Change PIN on first use required  
If this option is checked, the user will be required to change the PIN set in this dialogue to a new value during the first authentication.

Clear  
The Clear Button allows the administrator to remove any information or selections made and return the dialogue to the original state.

Set  
The Set Button activates the command and sets the new PIN.

Comment Field  
This section of the dialogue allows the Security Administrator to enter a free-form comment related to this action. This forms a permanent part of the token history and will be displayed in the Token detail dialogue.

Close  
The Close button ends the dialogue and returns control to the Secured User Tab.

Results  
This section of the dialogue provides the results of the set new PIN action.

Resync Button  
The Resync Button is available for tokens in an Active or Suspended state and is used to manually resync or confirm the proper operation of the token.

Note: BlackShield ID can automatically resync a token. Refer to Synchronization on page 84.

Highlight a token and click the Resync button to open the token Resync dialogue.
Instruct the user to key the challenge displayed in this dialogue into their token to generate a response. Key the response generated by the token into the Response field, then click Resync. The result group will indicate the result of the resync action. If resync succeeds the user will be able to authenticate using the token. If the resync fails, authentication will continue to fail.

A resync operation can fail for any of the following reasons:

- The serial number of the token does not match the serial number displayed in the dialogue.
- The challenge is incorrectly keyed into the token.
- The response is incorrectly keyed into the dialogue.

**Note:** the resync process does not require the user’s PIN. Only the passcode generated by the token should be keyed into the response field.

### Issue Button

The Issue button is used to activate software tokens that are in the Assigned state.

Select BlackBerry to email the initialization file to the selected user’s BlackBerry.

Select BlackShield MP to save the initialization file. By default the file will be stored in the Default File Location set on the Policy Tab. (Refer to Token File Location Group on page 94). This file will need to be
transferred to the users target device for import into the token software. The actual installation method will vary depending on the device. Refer to the MP software token user guide.

![Issue Token](image)

*Issue Token*

Issue a software token. Please select method to issue the token.

**Issue Method**

- BlackBerry
- BlackShield MP

**Result**

[Issue]

[Close]
Snapshot Tab

The Snapshot Tab groups functions that relate to authentication activity by users known and unknown to BlackShield. In general, functions related to system metrics and token status is grouped on the Snapshot Tab along with the user authentication information.

Figure 69 - Snapshot Tab

Authentication Activity Group

This group provides the information on Authentication activity against the BlackShield server. The default values for the group are for a start and end date of today, and a Result setting of All, so each time the Tab is accessed all actions for the day are displayed. The default number of records displayed is 100 which is also the maximum value allowed in this field. All the selectable fields work together to filter the results.
Start and End dates: The Start and End dates are used to select the period for display in the list of authentication attempts. The dates may be typed into the field or the calendar selected to allow a direct selection of the day required.

![Figure 70 - Start Date Calendar](image1)

![Figure 71 - End Date calendar](image2)

Results: The Results drop down list is used to select the Authentication results the Administrator would like to view in the list.

![Figure 72 - Authentication Result Selection](image3)

Sort: The Sort Button activates the command, filtering the authentication attempts for display in the table. The results may be resorted by selecting the column headers to view the records from the top down or bottom up.
Systems Metrics Group

This group provides the information on Authentication metrics, Token Status, and License Status for the system.

Authentication Metrics

The System Metrics group reports the total number of Authentication Pass (Success), Fail (Failure), and Total for the system as filtered by the time selection. Only Success and Failure results are counted in this statistic. The Administrator may select Today (default), Last Week, Last Month or Last Year. The results of these selections are as follows:

- Today – all Pass and Fail authentication attempts for the current 24-hour period from midnight to midnight.
- Last Week – all Pass and Fail authentication attempts for the previous seven days including today.
- Last Month – all Pass and Fail authentication attempts for the previous thirty days including today.
- Last Year – all Pass and Fail authentication attempts for the previous 365 days including today.
Token Status

This section of the System Metrics group reports on the current state of all tokens registered on the system. Tokens are sorted by type and totals are listed by: Inventory, Allocated, Assigned, Active, Suspended, Locked, Lost/Failed, Deleted, and Purged.

License Status

This section of the System Metrics group reports on the current state of the License and lists the License type, expiration date, and Available capacity.
License Types

A BlackShield ID license may be one of the following types: Evaluation, NFR, Limited, Permanent or ICE.

Evaluation Licenses are valid for a limited period of time to allow for end-to-end functionality testing prior to purchasing. An evaluation server may be converted to a fully licensed product by applying any other type of license.

NFR licenses may be issued to qualified partners for the purposes of testing and demonstration.

Limited Licenses sets a fixed start and stop date for the server.

Permanent licenses do not expire.

ICE licenses (In Case of Emergency) allows for a temporary increase in license capacity for a predefined amount of time. Please refer to Appendix E for additional information.

The remaining elements in this section list the licensed capacity by token type and the remaining capacity by token type. Each time a token is assigned to or revoked from a user the corresponding token capacity is decremented or incremented respectively.
Chapter 12 – Operators, Roles and Remote Management

By default remote management is disabled and only a user with an administrator account on the BlackShield ID localhost is able to manage the server. Once configuration is complete and security policies are established, remote management can be enabled and Operators can be created.

Operator Tab

The Operator Tab provides access to functions that are used to promote a Secured User to Operator status, assign roles and allow remote management.
Figure 75 - Operators Tab

Operator Create

Any user that has been issued a token or password for authentication against BlackShield ID can be elevated to Operator status.

Click the Search button to display a list of potential Operators. Refine the list using the options in the User Search Group.

Note: CRYPTOCard strongly recommends that token-based authentication be mandatory for all Operators. Static password authentication is supported but not recommended.

Highlight the user to be elevated, and then check the Operator Rights option box. This will enable the Access Control list. Check the tabs to which the Operator should have access. Note that the Remote Management tab must be checked to allow a remote browser-based management session.

Roles

The functions available through BlackShield ID UI are logically grouped on tabs. Roles can be created by allowing Operators access to only those tabs required to perform their designated tasks. The following represent typical configurations:

Help Desk

The following configuration allows help-desk operators to perform typical user support tasks. Specifically it prevents new tokens from being issued to users and any changes to Security Policy, other Operator accounts and System configuration.


Audit

The following configuration allows Auditors to generate reports on user, authentication and operator activity.

- Enabled tabs: Snapshot, Reports, and Remote Management.
Issuing Authority

The following configuration allows the Operator to import, initialize, assign and revoke tokens.

Enabled tabs: Snapshot, Secured Users, Assignment, Reports, and Remote Management.

Operator Activity

The Operator Activity group provides a list of recent actions performed by the Operator. A complete history of activity is databased and can be reviewed by running the Operator Activity Report available on the Reports Tab.
Chapter 13 - Reports

Reports Tab

The Reports Tab groups functions that relate to reporting on Tokens, Users, Operators and Authentications, as well as Token Summaries. Reports are generated by number of records rather than by date.

On-line Reports

The maximum range of data which can be reported through the Reports tab is determined by the settings in the Archive Group of the System Admin tab (refer to Archiving on page 76). Data that exceeds the maximum number of database rows or timeframe is automatically archived in .csv archive files.

On-line reports can be saved in either .csv or tab delimited file formats; either of which is readily imported into database, spreadsheets or common reporting tools.
System Summary Totals

This group provides the information on Tokens and their current state within the BlackShield ID application. The number of tokens Available, Assigned, Enabled (Active), Suspended, Revoked, and Lost are reported here and updated continuously.

Token Summary Totals

This group provides the information on the total number of Tokens initialized or imported into BlackShield ID. The number includes all Tokens in all states and may exceed the license capacity of the system. The KT and RB fields simply list the total number of each type of token that is currently in the system.

General Report Settings

This group provides the controls for limiting and selecting the Report file type that will be generated.

![Generated Report Settings](image)

The maximum number of records default value is 10,000 and may be changed to a larger or smaller number as required for the report being generated.

Tab Delimited or CSV file types are available and will result in flat files being generated in the respective formats for input into third party applications for display and analysis.

Reports

This list provides a list of available reports.
Figure 78 - Reports

1-Day Authentication – this report provides information on all authentication attempts for the last 24-hour period. Data is listed under headings for: Date, User Name, Serial Number, Source IP, Action, Result and Message.

30-Day Authentication – this report provides information on all authentication attempts for the last 30-day period. Data is listed under headings for: Date, User Name, Serial Number, Source IP, Action, Result and Message.

365-Day Authentication – this report provides information on all authentication attempts for the last 1-year period. Data is listed under headings for: Date, User Name, Serial Number, Source IP, Action, Result and Message.

7-Day Authentication – this report provides information on all authentication attempts for the last 7-day period. Data is listed under headings for: Date, User Name, Serial Number, Source IP, Action, Result and Message.

Active Tokens – this report provides information on all Active tokens. Data is listed under headings for: Serial Number, Token Type, User Name, In Service (date and time), Initialization Date, Activation Date, Last Used (Date and time), Result, Result Count, Pass Count, Fail Count, Last Fail (Date and time), State set date, State, and Message.
Inactivity Report – this report provides information on users that have not authenticated with their token for a specific period of time. Data is listed under headings for: Days Since Last Authentication, Last Authentication, User Name, Last Name and First Name. A user must have authenticated with their token at least once to appear in this report.

Lost Tokens – this report provides information on all Lost tokens. Data is listed under headings for: Serial Number, Token Type, User Name, In Service (date and time), Initialization Date, Activation Date, Last Used (Date and time), Result, Result Count, Pass Count, Fail Count, Last Fail (Date and time), State set date, State, and Message.

Operator Actions – this report provides an audit trail of Operator actions. Data is listed under the headings of Action Date, Operator Name, Local Admin, Class, Type, Result and Action Data.

Operators – this report provides a list of operators, permissions and last login time.

Secured User – this report provides information on all Users assigned a password or token. Data is listed under headings for: User Name, Auth Date, Start Time, End Time, and Last Auth.

Self-enrollment – this report provides information on all Reservations for Self-enrollment. Data is listed under headings for: Reservation ID, Reservation Start Date, Reservation End Date, User Used, and User Name.

Tokens By Serial – this report provides information on all tokens by serial number. Data is listed under headings for: Serial Number, Token Type, User Name, In Service (date and time), Initialization Date, Activation Date, Last Used (Date and time), Result, Result Count, Pass Count, Fail Count, Last Fail (Date and time), State set date, State, and Message.

Tokens by State – this report provides information on all tokens by current state. Data is listed under headings for: Serial Number, Token Type, User Name, In Service (date and time), Initialization Date, Activation Date, Last Used (Date and time), Result, Result Count, Pass Count, Fail Count, Last Fail (Date and time), State set date, State, and Message.

Reports Management Group

This provides the command to run the reports. The report button opens a File Download Open/Save/Cancel window. The selected report will be run and the number of records set will be generated into a tab delimited or CSV formatted file.
Figure 79 - Report Mgt Group

License Group

Clicking this button outputs the details of the currently installed BlackShield ID license, including type, date range and capacities.

![License Group](image)

Figure 80 - License Group

Figure 81 - Report File Download Dialogue

Open

Selecting Open will result in a Notepad window opening with the data displayed in text format. The file may then be saved for later review or as a source file for a third party reporting tool.

Save

Selecting Save will result in a normal windows Save As window opening where the destination directory may be selected and the file is saved.

Cancel

This simply returns control to the Reports Tab.
Chapter 14 - High Availability Solutions

BlackShield ID can be installed in a variety of configurations to protect against loss of service due to a hardware or network failure and to improve performance in high demand environments. In simple terms:

- The best protection against a network outage is to install two physically separated servers.
- Protection against hardware failures requires that critical processes be provided on 2 or more servers.
- Performance improvements can be achieved by separating processes and optimizing hardware to the needs of the process.

In a default installation, all of the BlackShield ID components are installed on the same hardware, though in most cases LDAP and web applications such as OWA and SharePoint are normally on separate hardware.

![Figure 82 - BlackShield ID Architecture](image)

In BlackShield ID terms, a site is defined as an instance of the BlackShield ID server. The number of sites that can be implemented is determined by the license installed on the Primary server. Multiple sites can share the same database, failover to an alternate database (one-way replication), distribute authentication processes across multiple databases, (multi-master replication) or be configured to use a database cluster.

Consider using dual core or quad core systems because BlackShield ID will automatically distribute CPU intensive operations across all available cores.

Single Location / Multi-site

The three main factors that can impact the overall performance of the system are peak authentication loading and operations such as report generation and authentication activity logging which are disk I/O intensive.

- Disk I/O performance can be improved by implementing the database on RAID 1+0 array.
- Moving components such as RADIUS, Self-enrollment and Self-service off the BlackShield ID authentication server will reduce CPU load, assuming these components are being used.
If the authentication loading exceeds the CPU resources of a BlackShield ID authentication server, implementing additional sites that use the same database can be beneficial. To estimate authentications per second, multiply the total number of sites by the authentication per second rate of a single site, bearing in mind that disk I/O and other management tasks may reduce the throughput. The actual number of authentications per second for a single site is hardware and resource dependant, however on recommended hardware approximately 100 authentications per second, per site, is a reasonable estimate.

Multi-location / Multi-site

Installing BlackShield ID sites in multiple locations protects against a network outage or catastrophic failure at a physical location. The recommended approach is to place a sufficient number of sites at the Primary (Location 1) and direct all authentication and management functions to this location. Only in the event of an outage are authentication and management functions automatically switched to the failover site. This type of configuration can be extended to support additional locations. It has the advantage of limiting the traffic generated by database replication and the network bandwidth required for replication and it reduces disk I/O.
Multi-location / Multi-site / Multi-master

Another alternative is to establish multi-master replication between two locations. Though a valid configuration, in most situations the traffic generated by replication and increase in disk I/O usually may negate the advantages of distributed processing. In most cases the configuration shown in Figure 86 - High Availability Multi-Location / Multi-site / Cluster on page 171 will outperform a multi-master configuration.
Multi-location / Multi-site / Cluster

Another option is to have multiple sites access a database cluster.

![Figure 86 - High Availability Multi-Location / Multi-site / Cluster](image)

Distributed Processing

In all cases with multiple sites, separating high disk I/O tasks such as auditing and reporting, from authentication processing, can also improve performance. In the following example, management tasks are handled by Site 3 while authentication tasks are distributed across Sites 1 and 2.
Virtualization

Depending upon the hardware, it may be practical to install sites inside virtual machines.

Any combination of these techniques can be used to achieve the desired availability and performance objectives. In most cases the configuration shown in Figure 86 - High Availability Multi-Location / Multi-site / Cluster on page 171 combined with virtualization will meet the needs of most organizations supporting up to 100,000 users.
Configure Sites and Replication

Establishing multiple sites follows the same implementation process, regardless of the High Availability architecture.

7. Configure the Primary site or reconfigure the Primary site whenever a change or addition is made to any of the following before adding or making changes to any other site:
   8. Database connection
   9. LDAP user data source connections
   10. Internal SQL user data source connections
   11. Export the Primary Site Key File and Configuration File
   12. Import the Primary Site Key File and Configuration File into all other sites

The number of permitted sites is determined by the license installed on the primary BlackShield ID server.

The Primary Server must be installed, configured and capable of processing authentication requests before installing and configuring additional sites.

Site Key and Configuration File

Before a Replica site can be configured, a site key and configuration file must be generated and exported by the Primary Server. This is done through the Sites button on the System Admin tab.

Site Export

Navigate to the System Admin tab and click the Sites button in the Actions group to open the Sites dialogue.
Figure 89 – Export Sites Dialogue

Ensure the Primary Server SQL database, LDAP user source and SQL user source configurations do not use a localhost or loopback IP address before continuing. All references must use host names or IP addresses.

13. Referring to Figure 89 – Export Sites Dialogue on page 174, select the Save button associated with the File Key (1) and click save on the File Download window. Save the file. A copy of this file will be required during installation of the replica. Control returns to the Sites window.

14. Select the Save button associated with the Site File (2) and click save on the File Download window. Save this file to the same location used in step 1.

15. These files are the only files that are required to create additional sites.

Install additional site(s)

Follow the instructions for installing a server. For multi-site configurations using the same primary database, install BlackShield ID using the custom option, declining installation of the default database.

When the installation is complete, logon to the replica server using a localhost administrator account. The administrator will be redirected to the System Admin tab.

Figure 90 - Import Sites Dialogue

16. Browse to the Site (1) configuration file exported from the Primary site and click Open.

17. Open the file containing the File Key from the Primary site and copy the key value into the File Key field. (2)

18. Click Load File (3)

19. Log out of the new site. From this point forward authentication and management functions can be performed at either site.
Figure 91 - Multi-site
Chapter 15 – System Backup and Restore

To backup or restore your BlackShield ID server system in the event of system or hardware failure, two steps must be completed prior to the occurrence of the failure event:

- A complete / full backup of the SQL database being used by BlackShield ID. Please refer to your database platform provider for the details on performing a backup of the database.
- The CipherExport tool must be run on all BlackShield ID servers to export its configuration, and the data output kept in a safe, secure location.

By default the BlackShield CipherExport tool is placed in the BlackShield ID server installation directory. For a default installation this path would be: <drive>\Program Files\CRYPTOCard\BlackShield ID\CipherExport.

To run the CipherExport.exe tool, open a DOS Command prompt and browse to the location of the CipherExport.exe file.

![Figure 92 - Cipher Export DOS Window](image)

At the command prompt enter this command:

```
CipherExport.exe export file_name.txt
```

where file_name.txt is the name you wish to call the output file (Ex. cipher-export.txt ). This file will be saved in the same directory location from which you run the CipherExport tool.

This command will create a file named ‘file_name.txt’ and display a key in the DOS Command prompt.

![Figure 93 - CipherExport Output](image)

Copy the value of the ‘Export File Key’ shown in the DOS Command prompt and save this into another text file (Ex. ExportFileKey.txt )
Take both text files, in this example it would be the ‘cipher-export.txt’ and the ‘ExportFileKey.txt’ to a secure and safe location as they are needed in order to restore a BlackShield ID server.

Note that the CipherExport tool must be run on each BlackShield ID server you have in use.

In the event of a system or hardware failure, to restore the BlackShield ID system to the same system or to a new system, you must use the CipherExport tool to import the BlackShield ID configuration. Following the new installation of BlackShield ID, to restore the configuration, you need to open a DOS Command prompt and browse to the location of the CipherExport.exe file.

Copy the ‘cipher-export.txt’ file to the same location as the CipherExport.exe tool on the new system. At the command prompt enter the following command:

\[
\text{CipherExport.exe import 'file\_name.txt' 'Export File Key value'}
\]

- Where ‘file\_name.txt’ is the name of the file created during the export. In this example ‘cipher-export.txt’.
- Where ‘Export File Key value’ is the value of the Export file key created during the export. In this example ‘2c31d27dfc0ff94081100178d045d’.

After the import command completes, you should see a message in the DOS Command prompt window that states ‘Cipher Imported’. Now login to the BlackShield ID console System Admin tab and continue with the configuration of the server.

Note that in order to completely restore the BlackShield ID server, a backup of the SQL database is also required.
**PostgreSQL Database Backup and Restore**

The default BlackShield ID PostgreSQL database should be backed up before attempting to upgrade or re-install BlackShield ID on another machine. During normal operation, it is recommended that a database backup be performed on a regular basis.

### Creating a backup of the BlackShield ID Database

The `pg_dump` command is used to create a database backup. This process can also be used to transfer a database from one BlackShield server to another.

2. Open a DOS prompt and browse to the `\Program Files\PostgreSQL\8.3\bin` directory.
3. Issue the command

   ```
   pg_dump -U username -v BlackShield_database_name > filename.sql
   ```

   **Example:**

   ```
   pg_dump -U postgres -v blackshield > blackshield.sql
   ```

   The database name is case sensitive. The default username is Postgres and the password is Password$.

4. When prompted for a password enter Password$ (default password) or the password you specified during the creation of the PostgreSQL user.
5. A sql file will be created in the `\Program Files\PostgreSQL\8.3\bin` directory. Copy it to a safe location.

### Restoring a backup of the BlackShield database

1. Stop the IIS Admin, World Wide Web Service and BlackShield Monitoring service.
2. Open a DOS prompt and browse to the `\Program Files\PostgreSQL\8.3\bin` directory.
3. Issue the command to enter the PostgreSQL interactive terminal.

   ```
   psql -U username
   ```

   **Example:**...
psql -U postgres

29. When prompted for a password enter Password$ (default password) or the password you specified during the creation of the PostgreSQL user.

30. If a Blackshield database already exists, type the command below, otherwise continue to Step 6.

   drop database blackshield_database_name;

   Example: drop database blackshield;

31. Issue the command

   create database database_name;

   Example: create database blackshield;

   (type \l to verify the database has been created then \q to quit.)

32. In the DOS prompt from the \Program Files\PostgreSQL\8.3\bin directory, issue the command

   psql -U username BlackShield_database_name < filename.sql

   Example: psql -U postgres blackshield < blackshield.sql

   The database name is case sensitive.

33. When prompted for a password enter Password$ (default password) or the password you specified during the creation of the PostgreSQL user.

34. Start the IIS Admin, World Wide Web Service and BlackShield Monitoring service.
Chapter 16 – Distributed Self-service / Enrollment Sites

The BlackShield ID Self-service and Self-enrollment web sites can reside anywhere in the network, provided they are able to connect to a BlackShield ID server. The web server that will host these sites must meet the same operating system and software requirements as for BlackShield ID.

Installing Remote Self-service / Self-enrollment Sites

- Create a Remote Services Key file or copy the exiting file from BlackShield ID (refer to Generate Remote Service Encryption Key File on page 73)
- Ensure that the IP address or Hostname of the BlackShield ID server can be resolved from the new server
- Ensure port 80/TCP is allowed from the Remote Site to the BlackShield ID server or whatever port you have configured your BlackShield web server to use for HTTP connections. Ensure port 443/TCP is allowed from the Remote Site to the BlackShield ID server or whatever port you have configured your BlackShield web server to use for HTTPS connections
- Run the installers

For 32 bit servers

<table>
<thead>
<tr>
<th>Service</th>
<th>Installer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Self-service</td>
<td>BlackShield ID Self-service.exe</td>
</tr>
<tr>
<td>Self-enrollment</td>
<td>BlackShield ID Self-enrollment.exe</td>
</tr>
</tbody>
</table>

For 64 Bit servers

<table>
<thead>
<tr>
<th>Service</th>
<th>Installer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Self-service</td>
<td>BlackShield ID Self-service x64.exe</td>
</tr>
<tr>
<td>Self-enrollment</td>
<td>BlackShield ID Self-enrollment x64.exe</td>
</tr>
</tbody>
</table>
Launch the site configuration tool (Start Menu | All Programs | CRYPTOCard | BlackShield ID [Service Name])

![Remote Site Configuration Tool](image)

**Figure 96 - Remote Site Configuration Tool**

- Click the Browse button to locate the key file which was downloaded from the BlackShield ID server. Once located, click the Open button. Once you have finished browsing for the key file, click the Apply button. Note: Once this keyfile has been loaded, it can be deleted from the browse to location.

- Within the first Location input box, enter in the IP or hostname of the primary BlackShield ID server. If you would like to specify a secondary BlackShield ID server to failover to, within the second Location input box, enter in the IP or hostname of the secondary BlackShield ID server. Then click the 'Specify failover BlackShield ID server' check box.

- Update the URL entries in the BlackShield ID server (System Admin tab; Self-service group, Self-enrollment group) to reflect the location of the remote sites.
Chapter 17 - Salesforce.com Delegated Authentication

BlackShield ID can be used to replace static password logon to the Salesforce.com web-based service.

The following are the implementation steps:

- Install the BlackShield ID component for Salesforce.com by running the BlackShield ID installer, select custom installation, and then select the salesforce.com component.
- Ensure that "Delegated Authentication" is enabled for the Salesforce.com
- Enter the URL of the BlackShield ID server.
- Ensure that "Delegated Authentication" is enabled for the Salesforce.com
- Enter the URL of the BlackShield ID server.
Chapter 18 - Customizing BlackShield ID

The following is a list of all customizable email template files (EMT) in BlackShield ID, and a brief description of their purpose. They are all installed to the Languages\en directory. The customer is free to change the text of these email template files to personalize them for their own organization. It should keep in mind that the XML tags inside the EMT files have special purposes. For example, every EMT file has <subject></subject> tags at the beginning. The text inside these tags is used for the subject line of the email. There are also <content></content> tags which are for the body of the email. Any other tags in the EMT file such as <dateTime/> or <name/> for example, are placeholders for details that are replaced by BlackShield before the email is sent out.

Note: the Languages\en directory is automatically overwritten during an upgrade or reinstall of the software. If customizing files, the recommended procedure is to create a new folder such as \Languages\custom and copy all files from the \Languages\en folder to this location. Make all modifications to files in the \Languages\custom folder. Finally, modify the windows registry settings for languages to reflect the new file locations:

![Figure 99 - Modify Language Settings for BlackShield ID](image)

Modify the Language key to reflect the new folder. (e.g. Change en to custom).

Follow the same procedures for modifying Agent language settings. Figure 100 - Modify Language Settings for Agents shows the registry settings for the Microsoft IAS/NPS RADIUS Component Agent.

![Figure 100 - Modify Language Settings for Agents](image)
EMT File List

- AuthServiceDown.emt – Used to report that the authentication service was found to be unresponsive during a scheduled check of the service.
- BlackberryPIN.emt – This is the content of the PIN delivery and management instructions for users that have been issued a software token for installation on BlackBerry.
- BlackberryToken.emt – This is the content sent with the software token initialization for users that have been issued a software token for installation on BlackBerry.
- EnrollmentLockout.emt – Used to report that a specific user was locked out of self-enrollment because of too many failed enrollment attempts.
- ExpiredReservation.emt – Used to report that a specific user did not enroll their token in time, and their enrollment reservation has been cancelled.
- iPhoneToken.emt – This is the email content sent to users who have enrolled an iPhone token.
- JavaMEOTA.emt – This is the email content sent to users who select the Over-the-Air deployment method during self-enrollment.
- JavaMEUSB.emt – This is the email content sent to users who select the option to install the Java Phone application using their third party phone vendor software.
- LicenseSpace.emt - Used to report that the available token capacity is getting low.
- LowDiskSpace.emt – Used to report that hard drive that BlackShield is installed on, is getting low on disk space.
- MailTest.emt – This is the email that is sent out to test the SMTP settings on the system tab.
- OperatorLockoutAlert.emt – Used to report to the operators that a specific user has had their account locked following too many successive failed login attempts.
- OperatorUnlockAlert.emt – Used to report to the operators that a specific user account has been unlocked.
- OrphanedToken.emt – This is the content sent as an email alert when a single token is orphaned.
- OrphanedTokens.emt – This is the content sent as an email alert when multiple tokens are orphaned.
- ReplacedUser.emt – This is the content send as an email alert when a UserID is changed and the account has an assigned token.
- SelfEnrollment.emt – Sent to the user as their invitation to self-enroll their hardware token. Provides them with enrollment instructions, a unique activation code, and a link to the self-enrollment website.
- stSelfEnrollment.emt – Sent to the user as their invitation to self-enroll their software token. Provides them with enrollment instructions, a unique activation code, and a link to the self-enrollment website.
- UserLockoutAlert.emt – Sent to the user to explain that their account has been locked following too many failed authentication attempts.
- UserUnlockAlert.emt – Sent to the user to explain that their account has been unlocked.
CLL Files

assignmentDynamic.ccl – modify the following entries in this file to change the SMS/OTP message content:

- 128=BlackShield ID<br>User ID: <USER_ID><br>Initial PIN: <PIN><br>TokenCode:<br><NEXT_OTP><br>OTP=PIN+TokenCode

Modifying Custom Fields

The Custom Field #1, Custom Field #2 and Custom Field #3 field labels appear on Assignment and Secured Users tabs. These labels can be modified by editing the assignmentStatic.ccl and securedUserStatic.ccl files respectively. Locate the Customer Field # entries in the file and replace with an entry of similar length.

Changes will appear in the UI after a restart of the BSID-Console application pool in the IIS Manager.
Appendix A – Upgrading from CRYPTOAdmin 5.32

The 5.32 migration tool is a command line utility to allow the import of users, tokens and groups from a 5.32 CRYPTOAdmin Server to the BlackShield ID server.

Migration prerequisites and limitations

- The 5.32 migration tool must be run on a BlackShield server already configured with an active database and user source connection (System Admin tab).
- Ensure that the license installed on BlackShield ID supports an equal or greater number of tokens as the CRYPTOAdmin 5.32 Server license, to ensure that all tokens are imported and activated for all users. If the number of tokens supported by the BlackShield ID license is smaller, the import and activation will not take place for any users, tokens or groups.
- The 5.32 migration utility requires an existing ODBC data source be configured on the BlackShield ID server to connect to the corresponding CRYPTOAdmin 5.32 database (i.e. MySQL ODBC data source configured on the BlackShield ID Server to connect to a MySQL database on the 5.32 CRYPTOAdmin server).
- The migration utility will not import operators, operator groups, hints, huntgroups, RADIUS attributes & clients, or peers file information. These must be manually created in BlackShield ID.
- CRYPTOAdmin 5.32 software tokens are imported and marked as version 5.x tokens (5.x Legacy token) in the database. Users with version 5.32 client software installed can authenticate against BlackShield ID without changing their client side software.
- BlackShield ID requires each token to have a unique serial number, whereas CRYPTOAdmin 5.32 server did not. If during the migration a duplicate serial number is detected, the migration utility will assign a new serial number to the token, and then assign it to the user. This change in the serial number does not affect a migrated users ability to authenticate against BlackShield ID.
- Serial initializers are not supported in BlackShield ID. Serial token initializers must be upgraded to USB token initializers.
- KT-1 tokens with serial number 3120xxxxx or earlier, and RB-1 tokens with serial number 2020xxxxx or earlier will be migrated into BlackShield ID but it might not be possible to reinitialize these token. These older tokens might need to be replaced with more recent models due firmware compatibility issues.
- Once the migration is complete, a migration log will be created in the \Program Files\CRYPTOCard\BlackShield ID\5-32-Migration\bin directory.
- If the BlackShield ID Server is configured to use LDAP, tokens are assigned and activated when the migration utility finds a match between the CRYPTOCard server token name and the LDAP user logon name. If a match is not found, the token is imported and placed in inventory.
Migration Steps

35. If using MySQL a grant statement must be added to allow connections from BlackShield to CRYPTOAdmin 5.x. Run the following statements on the MySQL server used by CRYPTOAdmin 5.x:

```sql
grant all privileges on *.* to root@IP_Address_of_BlackShield_Server identified by 'password';
grant all privileges on *.* to root@DNS_Name_of_BlackShield_Server identified by 'password';
grant all privileges on *.* to root@Hostname_of_BlackShield_Server identified by 'password';
flush privileges;
```

36. If using MySQL install the MySQL 3.x ODBC driver on the BlackShield server. The MySQL 3.x ODBC package can be found in the html, tools directory of the BlackShield ID distribution package. The MSSQL driver is included with Windows. The Oracle driver must be downloaded from the Oracle website.

37. On the BlackShield server launch Data Sources (ODBC) from Administrative Tools. In the System DSN tab add a new data source entry for the database server used by the CRYPTOAdmin 5.x server. This new entry will require a name, location of the database server, username, password and database name. The default database name is CRYPTOAdminjdbc.

38. On the CRYPTOAdmin 5.x server open the \Program Files\CRYPTOCard\CRYPTOAdmin\server\ccsecret file with a text editor. Make note of the uncommented text in the file (by default 123456).

39. On the BlackShield Server install the BlackShield ID 5.32 Migration Tool installation package.

40. Open a DOS prompt and browse to the \Program Files\CRYPTOCard\BlackShield ID\5-32-Migration\bin directory.

41. Run the BSIDMigrate532.exe command with the arguments required below

Usage: -odbc ODBC_NAME -secret SECRET [-batchsize size] [-v] -verbose

Example: BSIDMigrate532.exe -odbc CRYPTOAdminjdbc -secret 123456 -vv

-odbc ODBC_NAME

The name of the ODBC data source as configured in the Administrator Tools section of the control panel.

-secret SECRET
This is a required parameter. It is the text contained in the 'ccsecret' file on your CRYPTOAdmin server.

-batchsize size

Optional number to set the number of users and tokens to process in a single SQL call. Default value of 1000.

-v | -verbose

Turn on details to the console.

-vv | -veryverbose

Extra verbose. Includes Successful token imports. Will slow down the migration.

42. Verify that the migration log in the \Program Files\CRYPTOCard\BlackShield ID\5-32-Migration\bin directory contains no errors.
Appendix B – Upgrading from CRYPTO-Server 6.x

The 6.4 migration tool is a command line utility to allow the import of users, operators, tokens and groups from a 6.x CRYPTO-Server to the BlackShield ID server.

Migration prerequisites and limitations

- The 6.4 migration tool must be run on a BlackShield ID server already configured with an active database and user source connection (System Admin tab).
- Ensure that the license installed on BlackShield ID supports an equal or greater number of tokens as the 6.4 CRYPTO-Server licenses, to ensure that all tokens are imported and activated for all users. If the number of tokens supported by the BlackShield ID license is smaller, the import and activation will not take place for any user, operator, token or group.
- The 6.4 migration utility requires an existing ODBC data source be configured on the BlackShield ID server to connect to the corresponding 6.x CRYPTO-Server database (i.e. MySQL ODBC data source configured on the BlackShield ID server to connect to a MySQL database on the 6.4 CRYPTO-Server).
- The migration utility will not import RADIUS attributes and clients. These must be manually created in the BlackShield ID agent enabled IAS/NPS or Steel-Belted RADIUS software.
- CAP Protocol enabled agents are not support in BlackShield ID (CRYPTO-Logon, CRYPTO-Web and certain Citrix Web Interface agents). They must be updated to BlackShield ID agents.
- 6.4 CRYPTO-Server software tokens are imported and marked as version 6.x tokens (6.x Legacy token) in the database. Users with version 6.x CRYPTOCard Software Tools installed can authenticate against BlackShield ID without changing their client side software. This does not include CRYPTO-Server agents such as CRYPTO-Logon.
- If during the migration a duplicate serial number is detected, the migration utility will assign a new serial number to the token, and then assign it to the user. This change in the serial number does not affect a migrated user’s ability to authenticate against BlackShield ID.
- If the BlackShield ID Server is configured to use LDAP, tokens are assigned and activated when the migration utility finds a match between the CRYPTOCard server token name and the LDAP user logon name. If a match is not found, the token is imported but placed into inventory.
- Static password enabled users will not be enabled as static password users in BlackShield ID.
- KT-1 tokens with serial number 3120xxxxx or earlier, and RB-1 tokens with serial number 2020xxxxx or earlier will be migrated into BlackShield ID but it might not be possible to reinitialize these token. These older tokens might need to be replaced with more recent models due firmware compatibility issues.
- Serial initializers are not supported in BlackShield ID. Serial token initializers must be upgraded to USB token initializers.
Migration Steps

43. If using MySQL a grant statement must be added to allow a connection from BlackShield to the database server. Add the following statements to the MySQL server used by CRYPTO-Server 6.4:

```sql
grant all privileges on *.* to root@IP_Address_of_BlackShield_Server identified by 'password';
grant all privileges on *.* to root@DNS_Name_of_BlackShield_Server identified by 'password';
grant all privileges on *.* to root@Hostname_of_BlackShield_Server identified by 'password';
flush privileges;
```

44. On the BlackShield server install the ODBC driver required to connect to the 6.4 CRYPTO-Server database (MySQL, MSSQL or Oracle). The MySQL 5.x ODBC connector is included in the html, tools directory of the BlackShield ID distribution package. The MSSQL driver is included with Windows. The Oracle driver must be downloaded from the Oracle website.

45. On the BlackShield server launch Data Sources (ODBC) from Administrative Tools. In the System DSN tab add a new data source entry for the database server used by the 6.4 CRYPTO-Server. This new entry will require a name, location of the database server, username, password and database name. The default database name is CRYPTOAdmin6.

46. On the BlackShield server install the BlackShield ID 6.4 Migration Tool installation package.

47. Open a DOS prompt and browse to the \Program Files\CRYPTOCARD\BlackShield ID\6-4-Migration\bin directory.

48. Run the BSIDMigrate64.exe command with the arguments required below

Usage: -odbc ODBC_NAME [-org COMPANY_NAME] [-batchsize size] [-v|-verbose]

Example

```
BSIDMigrate64.exe -odbc CRYPTOserver -vv
-odbc ODBC_NAME

The name of the ODBC data source as configured in the Administrator Tools section of the control panel.
-odbc COMPANY_NAME

Optional name of the company in BlackShield that you wish the users and tokens to be
imported under.

-ca Attribute=Value

Optional custom ODBC attributes to pass to the ODBC data source when connecting

-batchsize size

Optional number to set the number of users and tokens to process in a single SQL call. Default value of 1000.

-v | -verbose

Turn on details to the console.

-vv | -veryverbose

Extra verbose. Includes Successful token imports. Will slow down the migration.

-u USER_NAME

Optional user name if the user name to connect with is not supplied in the ODBC connection.

-p PASSWORD

Optional password if the password to connect with is not supplied in the ODBC connection.

-oracle

Forces alternate SQL syntax to migrate from Oracle databases.

49. Verify the migration log in the \Program Files\CRYPTOCARD\BlackShield ID\6-4-Migration\bin directory contains no errors.
Appendix C – BlackShield ID Database Permissions

This appendix serves as a listing of all database permissions required for BlackShield ID during installation, normal operations, and during a server upgrade.

These permissions apply to all currently supported databases, including Oracle 10g / 11g, Microsoft SQL 2005 / 2008, MySQL 5.x, and PostgreSQL 8.x. Please refer to your database platform providers documentation on how to configure permissions for the database.

BlackShield ID – Installation and Normal Operations

Create Database (except for Oracle)
Create Table
Create Index
Create View
Insert
Select
Update
Delete

BlackShield ID – Upgrades

Create Table
Create Index
Create and Delete View
Select on
Oracle
  all_tab_columns
  user_ind_columns
MSSQL

INFORMATION_SCHEMA.KEY_COLUMN_USAGE
INFORMATION_SCHEMA.TABLE_CONSTRAINTS
sysobjects
syscolumns
sysindexes
sysindexkeys
sysconstraints

PostgreSQL

INFORMATION_SCHEMA.COLUMNS
INFORMATION_SCHEMA.KEY_COLUMN_USAGE
INFORMATION_SCHEMA.TABLE_CONSTRAINTS
pg_index
pg_class
pg_namespace
pg_tablespace

MySQL

INFORMATION_SCHEMA.COLUMNS
INFORMATION_SCHEMA.KEY_COLUMN_USAGE
INFORMATION_SCHEMA.TABLE_CONSTRAINTS
INFORMATION_SCHEMA.STATISTICS
Appendix D – In Case of Emergency (ICE) Licenses

A BlackShield ICE license allows for a temporary increase in license capacity for a predefined amount of tokens over a certain period. Tokens issued under the temporary ICE license are marked as “ICE” tokens. After the ICE license has expired, all tokens marked as ICE return to a suspended state and can no longer be used for authentication. Installation of a new BlackShield ICE license will allow you to reactivate tokens set to an ICE state.

Installing a BlackShield ICE License

Select the System Admin Tab. In the Licenses section click the Browse button and select the ICE enabled BlackShield License btk file. In the Activation Key section, enter the Activation key.

An “In Case of Emergency Capacity” section will appear under Licenses.

The ICE License capacity and duration can be found by selecting the Details button.

Tokens flagged as “Is ICE Token” can be assigned to users in advance but they cannot be used for authentication until the Activate button is selected.

After the ICE license has been activated the Start and End date can be seen on the License Status section of the Snapshot Tab.
Assigning ICE Tokens to users using Auto Provisioning

CRYPTOCard ICE tokens can be assigned and issued to users after installation but before activating the ICE license. The recommended procedure is to use self-enrollment, which confirms the installation of the token by the user. Allocation of tokens to a large group of users can be performed from the Provisioning Rules Settings section in the System Admin Tab.

The process is simple. Supply a name for the rule, select the token type, enable “Assign as ICE token” then select the Microsoft Group(s) for which the rule should apply.

The users within the selected Microsoft Group will receive a Self-Enrollment email (refer to page 116 for more in-depth information on Self-Enrollment). The Self-Enrollment email will walk them through the process of installing CRYPTOCard software (if required) and activating their CRYPTOCard token. The content of the self-enrollment email can be modified, refer to on page 183 for more information.
Assigning or Enrolling ICE Tokens on a per user basis

An ICE token can be assigned on a per user basis. In the Assignment Tab, perform a search for a user and token then select the Assign or Enroll button.

Place a checkmark in “Is ICE Token” then select Assign or Enroll.

The Enroll option sends a Self-Enrollment email to the user. The Self-Enrollment email will walk the user through the process of installing CRYPTOCard software (if required) and activating the CRYPTOCard token. The content of the self-enrollment email can be modified, refer to on page 183 for more information.

Expired ICE License

When a BlackShield ICE license expires, ICE tokens remain assigned to users but they can no longer be used for authentication. If users attempt to use their ICE token a message will appear in the Snapshot tab.

Ice tokens can be deassigned from users and placed back into inventory. This will revert the token back to a usable state.

BlackShield tokens placed in an Inventory, Initialize or Lost\Failed state do not consume BlackShield Server license capacity.