SafeNet Authentication Service

Welcome Guide

MP-1 BlackBerry

Document Information

Document Part Number	007-012424-002, Rev. A
Release Date	September 2013

Trademarks

Disclaimer

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

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

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

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

Contents

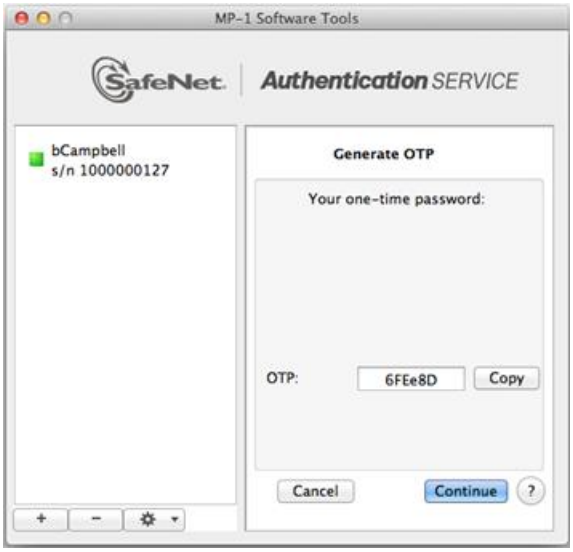
Overview

The BlackBerry is a wireless handheld which supports email, mobile telephone, text messaging, internet faxing, web browsing and other wireless information services. While including the usual PDA applications (address book, calendar, to-do lists, etc.), along with telephone capabilities on newer models, the BlackBerry is primarily known for its ability to send and receive e-mail. Armed with a SafeNet Authentication Service (SAS) token the BlackBerry can be used to log on to any SAS-protected network.

SAS supports three deployment methods:

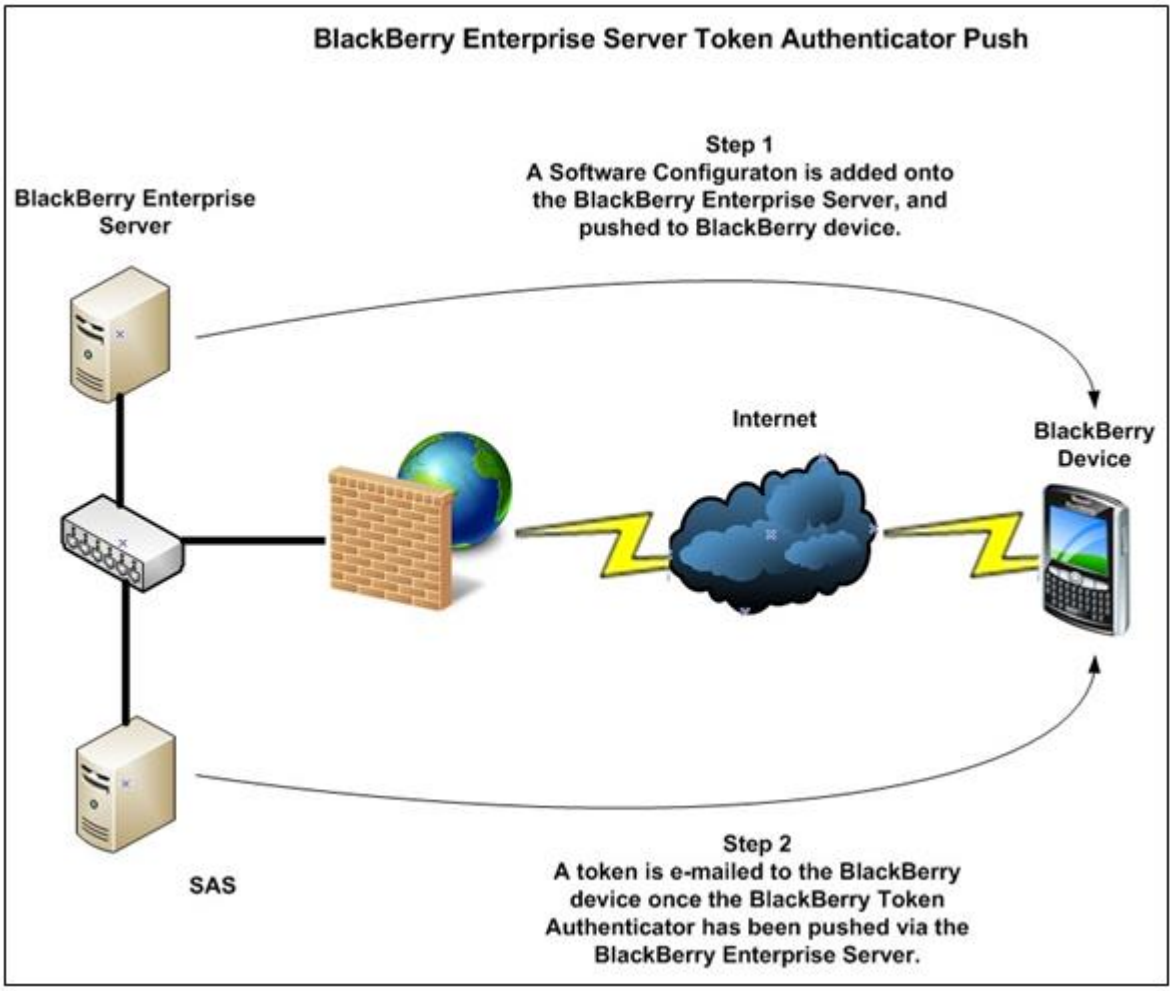
- BlackBerry Enterprise Server Deployment
- BlackBerry Desktop Manager (USB) Deployment
- SAS Server Deployment
- BlackBerry Enterprise Server Deployment

This guide provides instructions for installing and activating your SafeNet MP-1 software token. Once activated, you will use your MP-1 token every time you log on.



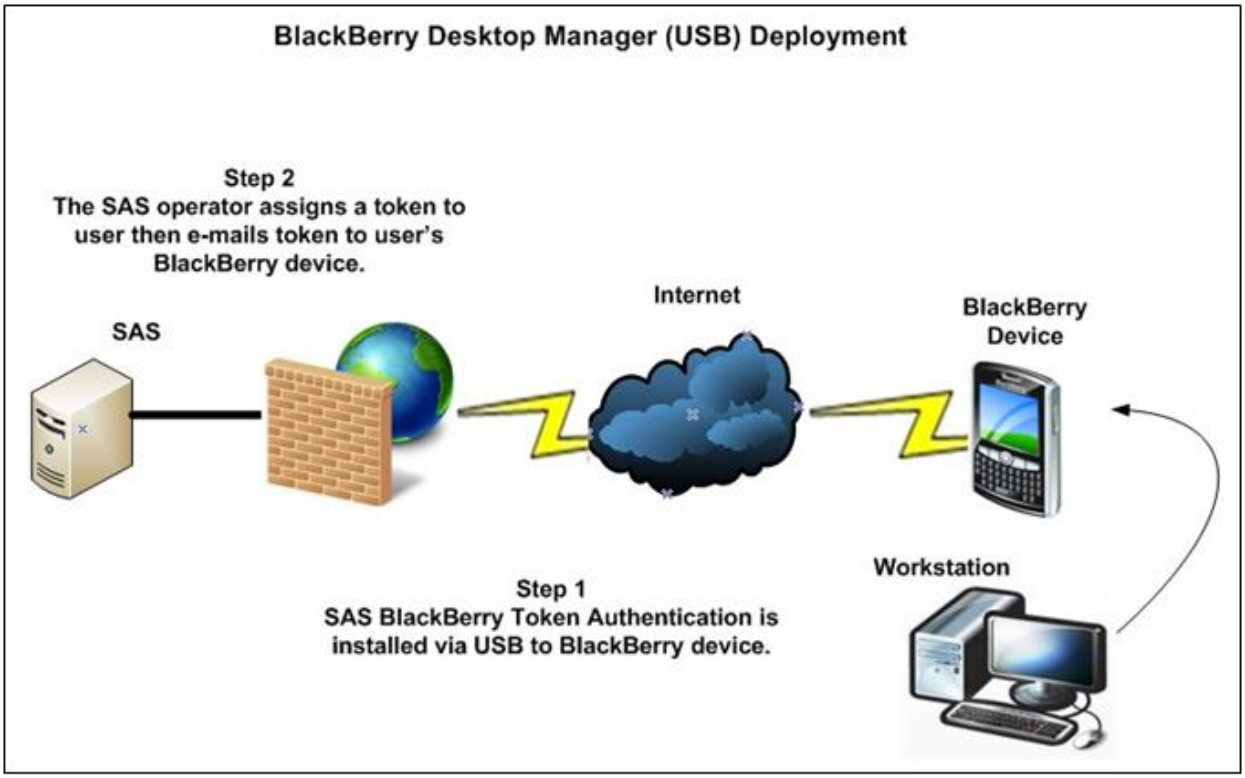
Until now, you've logged on with your user name and password. The problem is that passwords are easily compromised, putting your identity and the resources you access at risk. By using an MP-1 token for authentication, you will be able to generate a one-time password (OTP). As the name implies, an OTP can only be used once. Each time you log on, you will use your MP-1 to generate a new OTP.

BlackBerry Enterprise Server Deployment



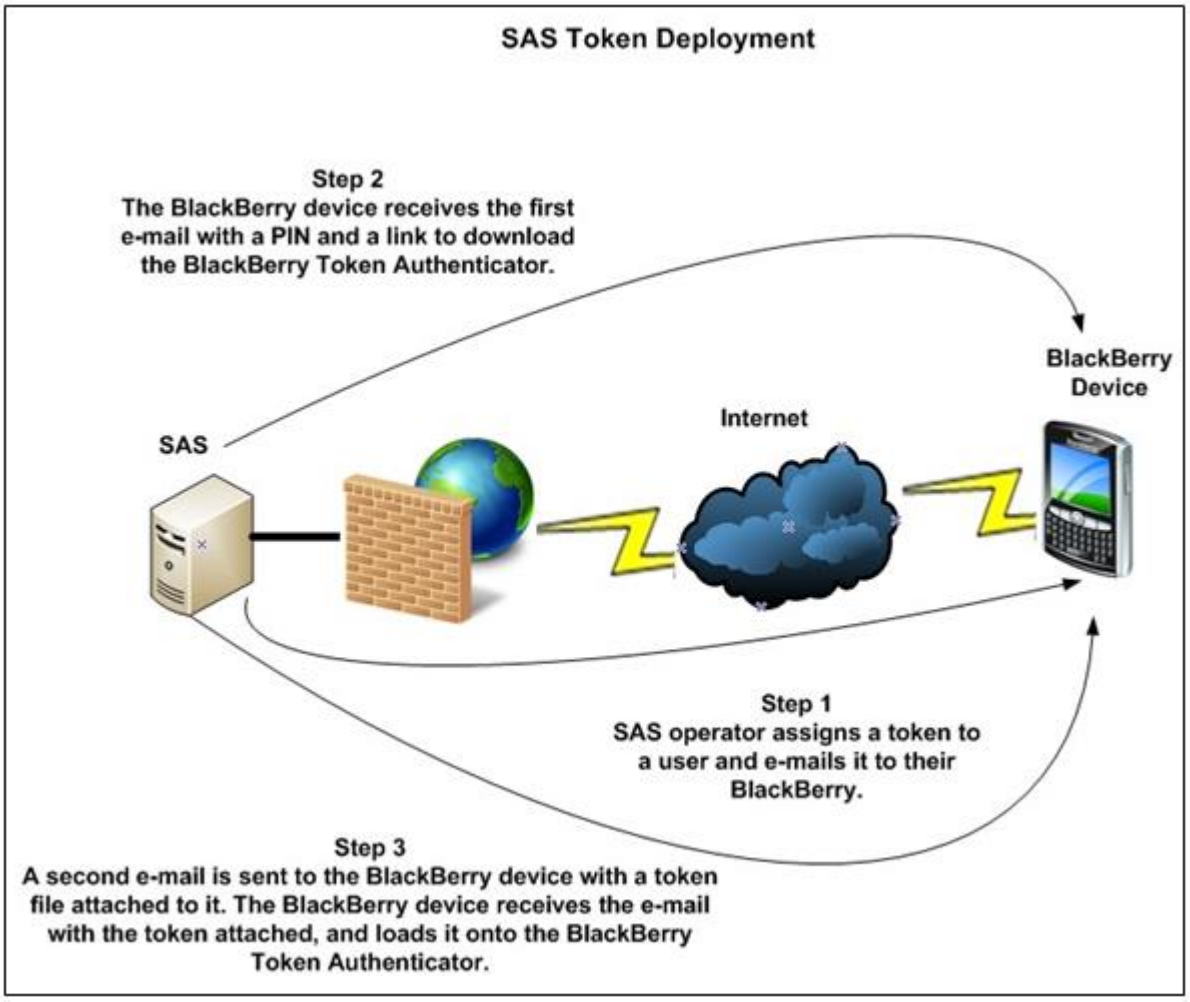
1. A SAS Software Configuration and IT policy is created on the BlackBerry Enterprise Server and pushed to the BlackBerry device.
2. The SAS Administrator assigns then issues or enrolls an MP token to the BlackBerry user. The user, via email, receives the PIN and SAS token or enrollment message then activates their SAS token.

BlackBerry Desktop Manager (USB) Deployment



1. The BlackBerry Token Authenticator Software and BlackBerry Token Attachment Handler are installed using the BlackBerry Desktop Manager.
2. The SAS Administrator assigns and then issues or enrolls an MP token to the BlackBerry user. The user, via email, receives the PIN and SAS token or enrollment message and then activates their SAS token.

SAS Token Deployment



1. The SAS Administrator assigns and then issues or enrolls an MP token to the BlackBerry user.
2. The BlackBerry user receives email containing a link to BlackBerry Token Authenticator Software, and a BlackBerry Token Attachment Handler and PIN.
3. The BlackBerry user receives a second email, which contains their token.
4. Alternatively, the user receives a self-enrollment email that includes a link to the Self- Enrollment website. The website will walk them through the process of activating their SAS token.

Configuration

BlackBerry Enterprise Server 4.x Deployment

Initial BlackBerry Enterprise Server 4.x Configuration

The following instructions provide the necessary steps in creating policies to push the BlackBerry Token Authenticator to a Blackberry device via a Blackberry Enterprise Server.

1. On the Blackberry Enterprise Server, navigate to the **C: \Program Files\Common Files\Research in Motion** directory. Create the following folder structure:
   - Create a folder called **Shared**.
   - Create a folder called **Applications** under **Shared**.
   - Create a folder called **SAS** under **Applications**.
2. On the SAS server browse to the **C: \Program Files\Cryptocard\BlackShield ID\BlackShield Site\blackshieldss\blackberry** folder.
3. Copy the following files into the **C:\Program Files\Common Files\Research in Motion\Shared\ Applications\ Cryptocard** directory on the BlackBerry Enterprise Server:
   - BBAuthenticator.alx
   - BBAuthenticator.cod
   - BBAuthenticator.jad
   - BBAuthenticator.jar
   - BBMailRun.alx
   - BBMailRun.cod
   - BBMailRun.jad
   - BBMailRun.jar
4. On the BlackBerry Enterprise Server, open up command prompt and navigate to **C:\Program Files\Common Files\Research In Motion\Apploader**. Enter the command: **loader.exe /index**
5. This will create files called **PkgDBCache.xml** and **specification.pkg** in the **C:\Program Files\Common Files\Research in Motion\Shared\Applications\Cryptocard** directory. Share the **Research in Motion** folder so the Blackberry Enterprise Server can access the files, and leave the permissions to the default settings.

Adding SAS Applications to the BlackBerry Enterprise Software Configuration

1. Log in to your Blackberry Enterprise Server, highlight the Blackberry Domain (root level), and then select **Software Configurations**.
2. Choose **Add New Configuration** then select **Change**.
3. In the **Device Software Share Location**, enter: **\<hostname>\Research in Motion**
4. Select **OK**.
5. Create a policy to allow the installation of **BBAuthenticator** and **BBMailRun**. Click **New**.
6. Enter a description in the **Name** field.
7. Change **Disposition** to **Required**, and then click **OK**.
8. Expand **Application Software**.
9. In the **Delivery Column**, select **Wireless** for **BBAuthenticator** and **BBMailRun**.
10. In the **Policy** column, allow the installation of **BBAuthenticator** and **BBMailRun**, and then click **OK**.

Creating an IT Policy

1. Select the Blackberry Domain (root level), and then click **Global**.
2. Select **Edit Properties > IT Policy > IT Policies**. Create a new IT Policy, which will allow the installation of the SAS applications onto the BlackBerry device(s).
3. Select **Security Policy Group**.
   - Set **Disallow Third Party Application Download** to **False**.
   - Set **Allow Third Party Apps to Use Persistent Store** to **True**.
4. Select **OK** until all windows are closed.

Assigning and Deploying a Software Configuration and IT Policy

1. Launch the BlackBerry Manager and select the BlackBerry server.
2. Select a BlackBerry user.
3. Expand the **Device Management** pane.
4. Select **Assign Software Configuration**.
5. Choose the SAS software configuration and then select **OK**.
6. Expand the **IT Admin** pane and then select **Assign IT Policy**.
7. Choose the IT Policy that allows the download of third-party applications and then select **OK**.
8. In the **IT Admin** pane, select **Resend IT Policy**. The IT Policy may take several minutes to take effect.

BlackBerry Enterprise Server 5.x Deployment

Initial BlackBerry Enterprise Server 5.x Configuration

To create and share the application folder, complete the following steps:

1. On the BlackBerry Enterprise Server, go to **C:\Program Files\Common Files\Research In Motion**.
2. Right-click the **Research In Motion** folder and select **Properties**.
3. Click the **Sharing** tab. Click **Share this folder** and then select **Permissions**.
4. Check **Full Control** (including **Change** and **Read access**), and then close the **Permissions** window.
5. On the Blackberry Enterprise Server, navigate to the **C:\Program Files\Common Files\Research in Motion** directory. Create the following folder structure:
   - Create a folder called **Shared**.
   - Under the **Shared** folder, create a folder called **Applications** under Shared.
6. On the SAS server browse to the **C:\Program Files\Cryptocard\BlackShield ID\BlackShield Site\blackshieldss\blackberry** folder.
7. Copy the following files into the **C:\Program Files\Common Files\Research in Motion\Shared\Application**s directory on the BlackBerry Enterprise Server:
   - BBAuthenticator.alx
   - BBAuthenticator.cod
   - BBAuthenticator.jad
   - BBAuthenticator.jar
   - BBMailRun.alx
   - BBMailRun.cod
   - BBMailRun.jad
   - BBMailRun.jar

Adding SAS Applications to the Software Configuration

1. In the BlackBerry Administration Service, in the left-pane, expand **BlackBerry Solution Topology**, expand **BlackBerry Domain > Component View**.
2. Select **BlackBerry Administration Service**.
3. Scroll to the bottom and select **Edit Component**.
4. In the **Software Management** area, in the textbox next to **BAS Application Shared Network Drive**, type **\\<hostname>\Research in Motion**.
5. Select **Save all**.

Adding/Publishing Application

1. In the left pane, under **BlackBerry solution management**, expand **Software > Applications**.
2. Select **Software Add or Update Applications**.
3. Browse to the SAS BlackBerry files at **C:\Program Files\Common Files\Research In Motion\Shared\Applications** and then click **Next**.
4. Click **Publish Application**.
5. Confirm that a new folder exists for the application under **C:\Program Files\Common Files\Research In Motion\Shared\Applications**.
6. Confirm that **PkgDBCache.xml** and **Specification.pkg** exist in this new folder.

Software Configuration via BlackBerry Solution Management

1. In the left pane, expand **Software > Applications**.
2. Select **Create a software configuration**.
3. Enter the name of the software configuration.
4. Set the **Disposition for unlisted Applications** to **Optional**. Click **Save**.
5. Click **View Software Configuration List** and select your new software configuration.
6. Click **Edit software configuration**.
7. Click the **Applications** tab.
8. Click **Add Applications To Software Configuration > Search**.
9. Select the check box beside the name of the new software configuration application.
10. Set the **Disposition** to **Required** or **Optional**.
11. Set the **Deployment** to **Wireless**.
12. Verify the **Application control policy** is set to **Standard Required**.
13. Click **Add to Software Configuration**.
14. Click **Save All**.

Configure Application Deployment Schedule

1. In the left pane, under **Devices**, expand **Deployment jobs**.
2. Click **Specify Job Schedule Settings**.
3. Click **Edit Job Schedule Settings**.
4. Set the **Default Delay** to **1 minute** (this can be left as default).
5. Click **Save All**.

Assign Software Configuration to User

1. In the left pane, under **BlackBerry solution management**, expand **User**.
2. Click **Manage Users > Search**.
3. Click on a user account.
4. Click on the **Software Configuration** tab.
5. Click **Edit User**.
6. Under **Available software configurations**, select the software configuration and then click **Add**. It should now appear under **Current Software Configurations**.
7. Click **Save all**.

Viewing Status of a Job

After you assign a software configuration to user accounts or change an existing software configuration that you assigned to user accounts, the BlackBerry® Administration Service creates a job to deliver BlackBerry® Device Software, BlackBerry Java® Applications, or application settings to BlackBerry devices.

If you assign an IT Policy to user accounts or change an existing IT Policy, a job sends the IT Policy changes to the BlackBerry devices. You can view the status of a job to determine if it is ready to run, currently running, completed, or completed with task failures.

1. In the left pane, under **Devices**, expand **Deployment jobs**.
2. Click **Manage deployment jobs**.
3. Click **Search for a job**.
4. In the search results area, under the **Status** column, you can view the status of the job.
5. To view more information about a job or to change a job, click the job ID.
6. Verify the application is installed on the device by clicking **Options > Advanced Options > Applications** on the BlackBerry device.

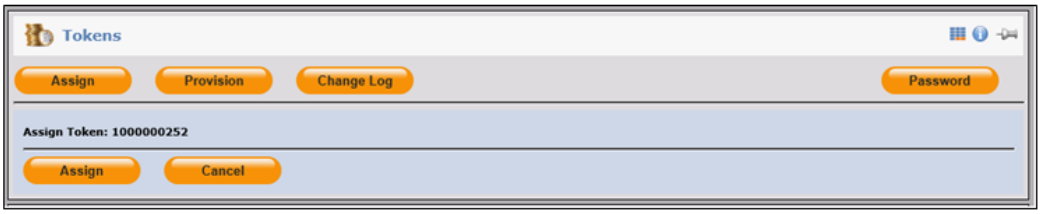
Deploying the SAS Token

SAS BlackBerry tokens are deployed to users via email. BlackBerry users will receive two email messages; the first email contains a SAS software download URL and the initial PIN to activate their token. The second email contains the SAS token.

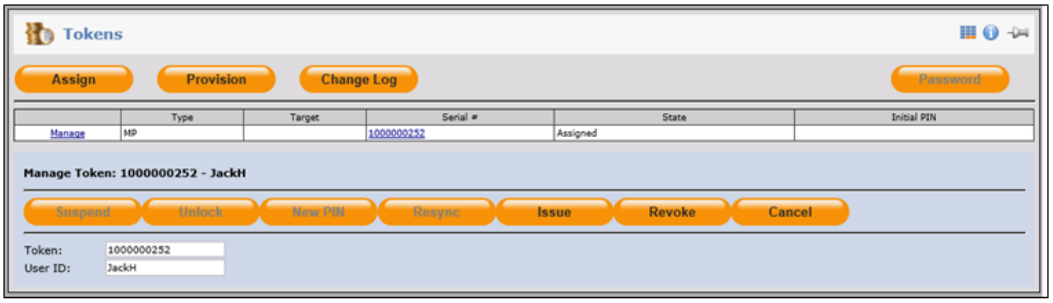
The content of each email is customizable; the URL link to the SAS software should be removed from the template. Refer to the Customizing the BlackBerry deployment email section for more information.

To deploy the SAS token:

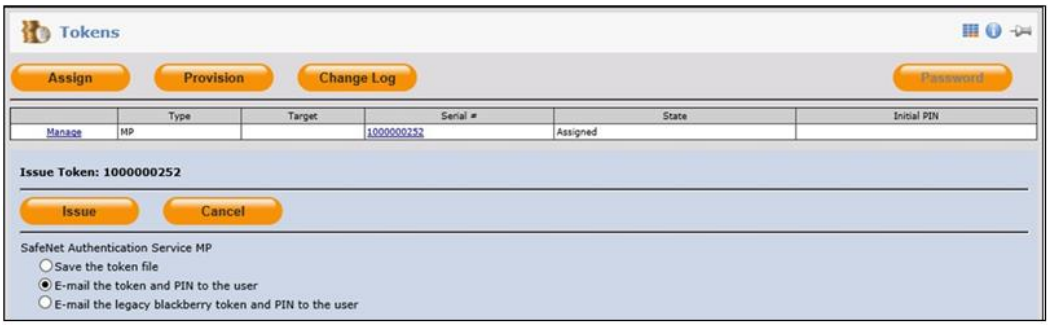
1. On the **Assignment** tab, find a user.
2. Select the user and click **Assign**.
3. Select the MP token and click **Assign**.



4. On the **Tokens** tab, select **Manage** (for the assigned MP token), and click **Issue**.



5. Select **Email the token and PIN to the user**.



6. Click **Issue**.

In the first email, make note of the initial PIN used to load the SAS token into the BlackBerry Authenticator. In the second email, scroll down to the token file at the bottom of the email and then select the **Load Token menu** option. This will launch the installation wizard. Enter the PIN to install the token.

The BlackBerry device may now be used to log on to a SAS-protected resource.

BlackBerry Desktop Manager (USB) Deployment

The following instructions provide the necessary steps to install the SAS BlackBerry Authenticator using the BlackBerry Desktop Manager.

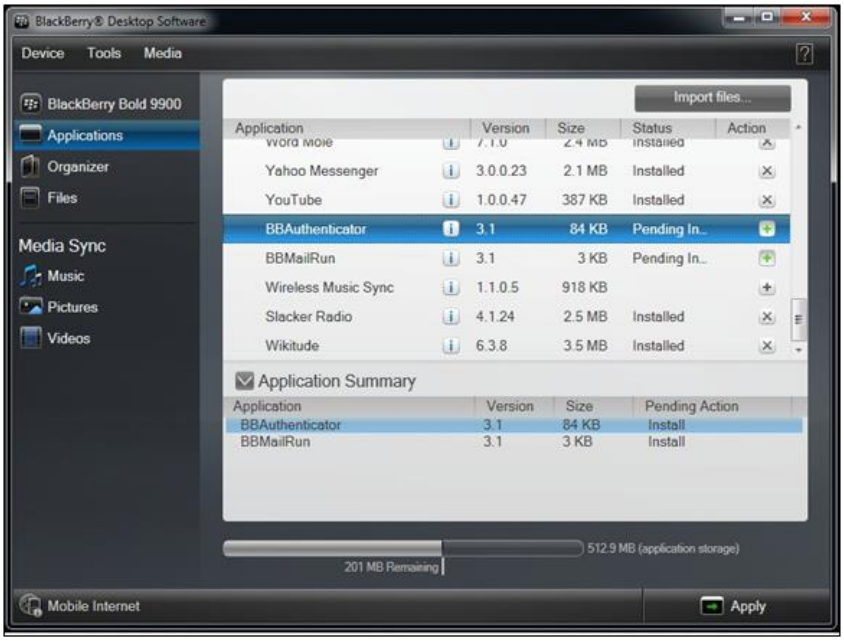
1. On the SAS server, browse to the **C:\Program Files\SAS\BlackShield ID\BlackShield Site\blackshieldss\blackberry** folder.

   The end user must be provided with the following files:

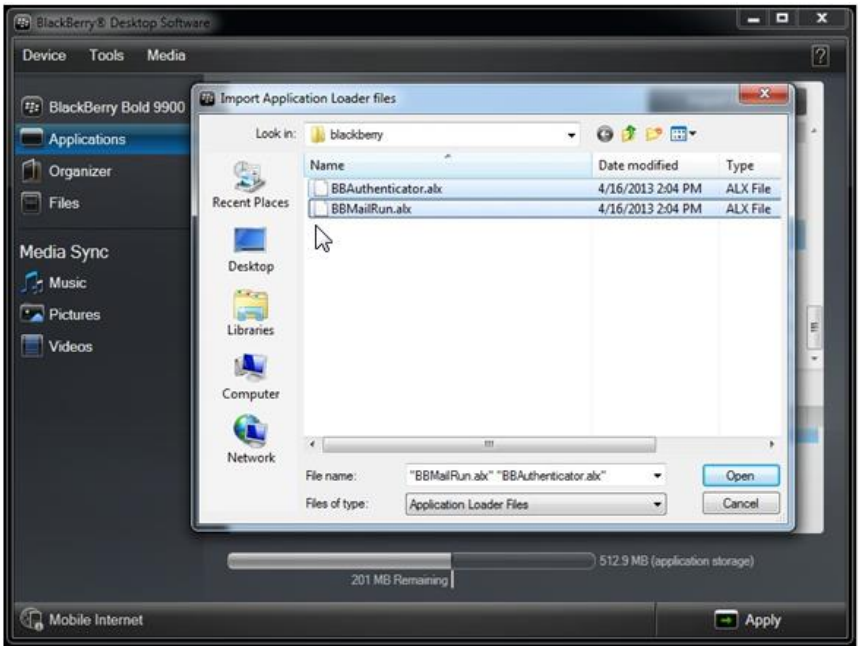
   - BBAuthenticator.alx
   - BBAuthenticator.cod
   - BBAuthenticator.jad
   - BBAuthenticator.jar
   - BBMailRun.alx
   - BBMailRun.cod
   - BBMailRun.jad
   - BBMailRun.jar

   Note: When installing an application for the second time, ensure all the relevant app files are located in the same directory where the previous version was saved (i.e. the location where you first saved the application).

2. Launch the BlackBerry Desktop Manager, and open the Application Loader.
3. Click the **Start** button in the **Add/Remove Applications** section to install SAS software.



4. Browse and select the **BBAuthenticator.alx** and **BBMailRun.alx** files.



5. The **Application Loader Wizard** will display BBAuthenticator and BBMailRun. (**Note:** The BBAuthenticator is dependent on BBMailRun.)
6. Click **Apply** to complete the installation of BBAuthenticator and BBMailRun onto the BlackBerry device.

SAS Server Deployment

Deployment of the SAS BlackBerry Authenticator can be used if an organization does not have a BlackBerry Enterprise Server or the ability to deploy via USB.

SAS server deployment method is limited by the restrictions imposed by BlackBerry Service Providers. Various providers do not allow the installation of third-party products. Please consult with your BlackBerry Service Provider for more information.

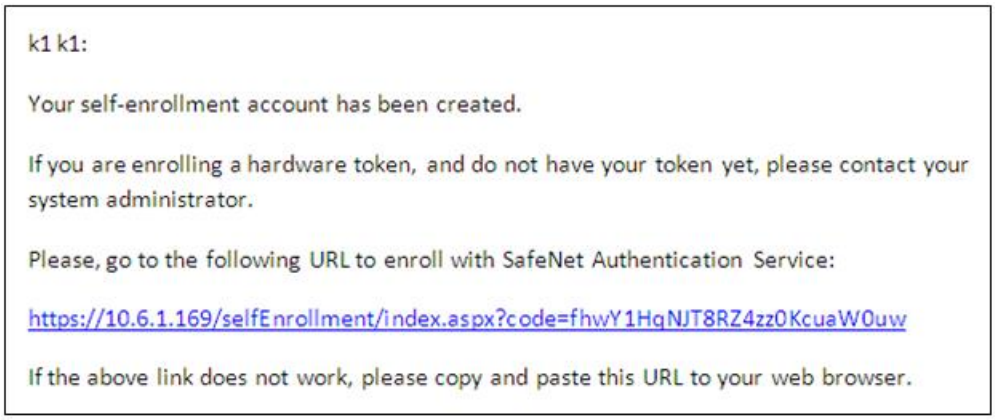
Configuring the Self Service URL

1. In the SAS Management Console, select the **Self Service** tab (under **Config Self Service**). Change the **Self Service URL** entry so it contains an external DNS or IP address entry.

   Note: Do not remove **BlackShieldSS** from the URL. **HTTPS** can be specified if the IIS web server contains a valid SSL certificate.

2. Click **Self Service Policy**.

3. Modify your firewall to direct HTTP traffic (TCP port 80) to the SAS ID server. HTTPS traffic (TCP port 443) can also be directed to the SAS server if a certificate exists on the IIS Web Server.
4. Upon deployment, the users first email message will contain a URL allowing them to download the required SAS software.



Customizing the BlackBerry Deployment E-mail

The BlackBerry email templates can be found in the **Program Files\Cryptocard\BlackShield ID\Languages** directory.

The **BlackberryPIN.emt** file contains information on where to download the SAS BBAuthenticator and BBMailRun software. It will also include the initial PIN used during the installation of the token. The **BlackberryToken.emt** file contains SAS BlackBerry token installation instructions.

The end user will receive these two email messages when a BlackBerry token is issued. The content can be modified to suit your organizations requirements.

The first email will include the following information: 1. A link to download the SAS BlackBerry Authenticator (BBAuthenticator) and Token Attachment Handler application (BBMailRun). 2. Their initial PIN.	BlackberryPIN.emt <subject>BlackShield ID Blackberry PIN</subject> <content><firstName/> <lastName/>: This e-mail will assist you in the installation and activation of your new SAS token into your Blackberry. Step one is to install the Token Authenticator and Token Attachment Handler application on your BlackBerry, step two is the installation and activation of the actual token. Please make note of the PIN below, as it is required to activate your token. To install the Token Authenticator "Over the Air", browse to the URL below with your BlackBerry. If the application is installed via Desktop Manager (USB) or Blackberry Enterprise Server, this step is not necessary. Again, please make note of your token activation PIN. Your token will be issued to you shortly. <blackberryURL/> Your token activation PIN is: <tokenPIN/> </content>
The second email will include the following information: 1. Token file to load into the BlackBerry	BlackberryToken.emt <subject>BlackShield ID Blackberry Token</subject> <content><firstName/> <lastName/>: Your new SAS BlackBerry token is attached. To install the token, move the cursor to the attached file. Click the trackwheel or trackball and then select the “Load Token” option on the menu. It will pop up the SAS BlackBerry token installation wizard and prompt for the user name and activation PIN. Use the activation PIN received in the previous e-mail. If you have not received an activation PIN, contact your Help Desk. </content>

Users must have the **Token Attachment Handler** application (BBMailRun) installed on the BlackBerry before receiving their token. If the user does not have this application installed prior to receiving the token, they will not see the **Load Token** option when they click on the Token Attachment.

To work around this, re-issue the token after the user has installed the Authenticator.

BlackBerry Token Functionality

BlackBerry token functions include:

- Generate a SAS One-time Password
- Challenge Response Mode
- Change PIN
- Token Resync
- Unlock Token
- User Preferences

Generate a SAS One-Time Password

Select the **Token Code** button. The application displays 1 of 5 options:

- **PIN Dialog:** This is the standard. The **PIN** dialog allows the user to enter in their token PIN. With the correct PIN, the token password is displayed in the white space below the SAS logo. With multiple unsuccessful PIN attempts, the token locks. Tokens cannot be unlocked unless the unlock option has been enabled with the properties of the MP token template.
- **Change PIN Dialog:** This is displayed if the token is in Change PIN mode.
- **Challenge Dialog:** This is displayed if the token is in **Challenge-Response** mode.
- **Unlock Token Dialog:** Allows an end user to enter an unlock code to re-enable their token.
- **Nothing is displayed:** A token has yet to be loaded into the application.

Challenge Response Mode

In challenge-response mode, the challenge/PIN dialog is displayed: With an incorrect PIN, the token displays an error box. With a correct PIN and incorrect challenge, the token displays the one-time password, but the token is out of sync. As a result, you need to re-synchronize the token to get a correct one-time password.

With the correct PIN/challenge, the token displays the correct one-time password.

Change PIN

To change the token PIN:

1. Select the **Options** button.
2. Select the **Change PIN** option.
3. On the **Change Token PIN** window, enter the current PIN, and then enter the new PIN twice to confirm it.

Token Resync

To re-synchronize the token:

1. Select the **Options** button.
2. Select the **Resync** option. The **Resync** window is displayed.

3. Enter the current PIN and the challenge provided from the **Secured User** tab, **Resync** button on the SAS Server. The one-time password is displayed.
4. Enter the one-time password into the **Response** section of the **Test/Resync Token** window and then select **Resync**.

Unlock Token

To unlock the token:

1. Select **Options > Unlock Token**.
2. Provide the unlock code to the SAS Server Administrator.
3. The SAS Server Administrator will provide a Server Response.
4. Enter the response in the **Server Response** field and select a new PIN.

User Preferences

To modify the disable numeric PIN fields:

1. Select **Options > Preferences**.
2. Clear the **Always use numeric PIN** check box.

Support Contacts

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

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