SafeNet | *Authentication SERVICE*

Welcome Guide for
MP-1 Token for Microsoft Windows

Protecting Your On-line Identity

Authentication Service Delivery Made EASY™

Support

SafeNet technical support specialists can provide assistance when planning and implementing SafeNet Authentication Service. In addition to aiding in the selection of the appropriate authentication products, SafeNet can suggest deployment procedures that will 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.

SafeNet works closely with channel partners to offer worldwide Technical Support services. If you purchased this product through a SafeNet channel partner, please contact your partner directly for support needs.

To contact SafeNet Authentication Service support directly:

Europe / EMEA	
Freephone:	0800 694 1000 (UK)
Telephone:	+44 (0)1276 608 000 (Int'l)
E-mail:	sassupport@safenet-inc.com

North America	
Toll Free:	800-307-7042
Telephone:	+1 613 599 2441
E-mail:	sassupport@safenet-inc.com

Publication History

Date	Description	Revision
2012.06.30	Updates to reflect SafeNet branding.	1.1
2011.05.06	Initial release	1.0

Contents

Welcome

Your company has chosen SafeNet Authentication Service Cloud Managed Authentication Service to help you protect your on-line identity and the networks, applications and data you use from unauthorized access.

In this package you will find instructions for installing and activating your MP-1 token. Once activated you will use your MP-1 token every time you logon.

Figure 1: MP-1 Software Token for Windows

What is a MP-1 Software Token?

Up 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 a MP-1 you will be able to generate a "One-time Password" or "OTP". As the name implies, an OTP can only be used once. Each time you logon you will use your MP-1 to generate a new OTP.

How does it protect me?

Password theft is the single most common way thieves and hackers steal identities and gain unauthorized access to networks and resources. While they have many ways to steal a password, success depends on the stolen password being valid, much the way credit card theft relies on the card being usable until you report it as stolen. The problem of course is that it is almost impossible for you or the security professionals that manage your network to discover your password has been compromised until long after damage has been done.

The MP-1 solves this problem because the instant you logon with your OTP, it is no longer valid. Any attempt to logon by reusing the OTP will not only fail, but also instantly alert your network security professionals to a possible attack on your identity.

Can anybody use my MP-1?

Your MP-1 is protected against unauthorized use by a Security PIN only you know. Again, much like a bank card or “Chip and PIN” credit card, the thief not only needs access to your MP-1 but must know your PIN as well. Any attempt to use the MP-1 with and incorrect PIN will fail. Successive attempts to guess your PIN will automatically “Lock” your MP-1, effectively disabling it, giving you and your network security professionals time to deal with the threat.

How does it work?

Each time you need an OTP, the MP-1 will prompt you to enter your Security PIN. For example:

Security PIN	OTP
1427	48466628
1427	4Kz6371R
1427	669-9487

How do I create a Security PIN?

You have or will shortly receive a “Self-enrollment Email” from your company which contains a unique URL to the self-enrollment web site and instructions for installing the MP-1 software, enrolling and activating your token. You will create a Security PIN that only you know during self-enrollment.

What is Self-Enrollment

Self-enrollment is a simple process for activating your token and creating your PIN. When you complete this process you will be able to use your token when you logon.

I have not received an Enrollment E-mail

If you have not received your self-enrollment email, contact your security administrator to arrange for a new self-enrollment email to be sent to you.

The Self-enrollment process

The process begins when you receive your self-enrollment e-mail notification containing instructions and an enrollment URL.

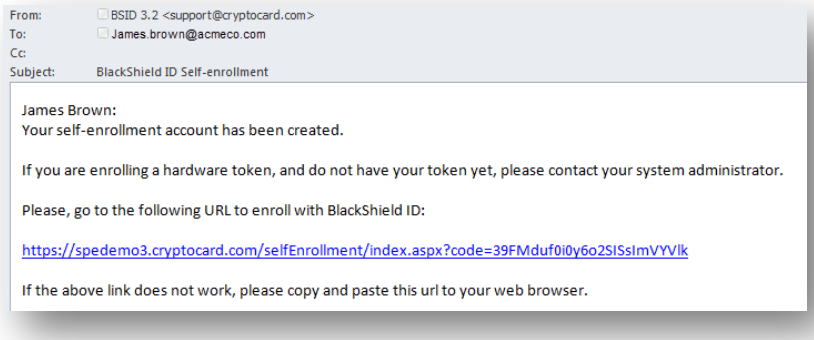


Figure 2: Example Self-enrollment e-mail

Step 1:
Read the instructions then using a browser, navigate to the URL in the message.

The enrollment web site will display a list of devices or "Targets" approved by your security administrator such as iPhone, Android, Blackberry and laptops upon which the MP-1 can be installed.

Choose the "Install Locally" option to load the token to the hard drive of your Windows computer. then click the "Next" button.

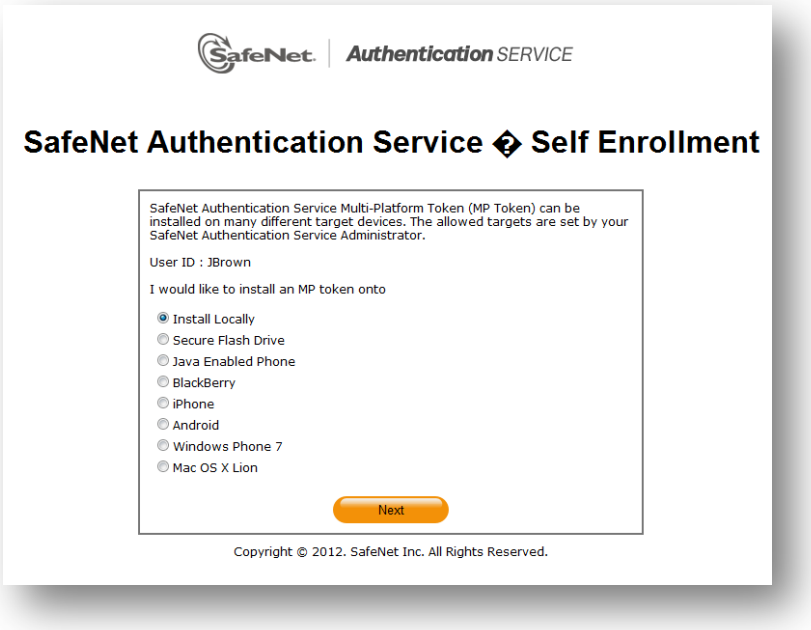


Figure 3: Select Install Locally to install on Windows

Step 2:
The next page displays links to download and install the MP-1 application called “Software Tools”.

Choose the x86 or x64 option for 32-bit or 64 bit Windows operating systems respectively. Complete the installation by following the on-screen instructions, then click “Next” to continue.

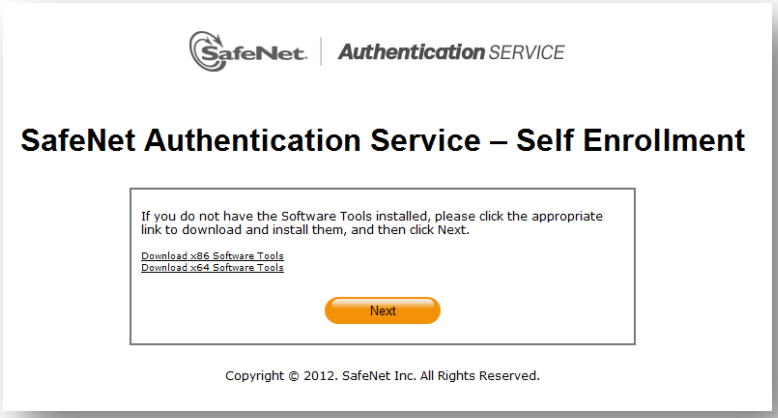


Figure 4: Confirm Enrollment Delivery Address

Step 3:
Depending on your browser configuration you may be prompted to download the token file. If so, click the “Download” button and save the file to your desktop, then click “Next” to continue. If you were not prompted, go to Step 4.

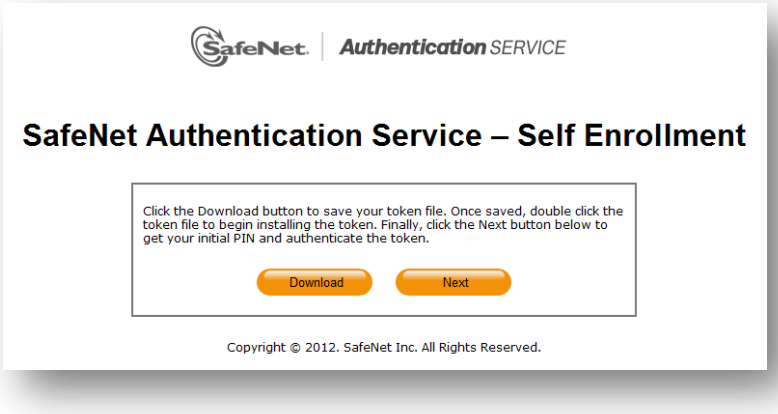


Figure 5: Download Token File

Minimize your browser, then locate and double-click the MP token file you saved to your desktop (.7mp extension).

Step 4:
The MP-1 application will now load the MP token file. To complete the process you will be prompted by the MP-1 application to provide the PIN displayed in your browser.

Be sure to memorize this PIN value.

Enter the PIN then click the “OK” button in the MP-1 application.

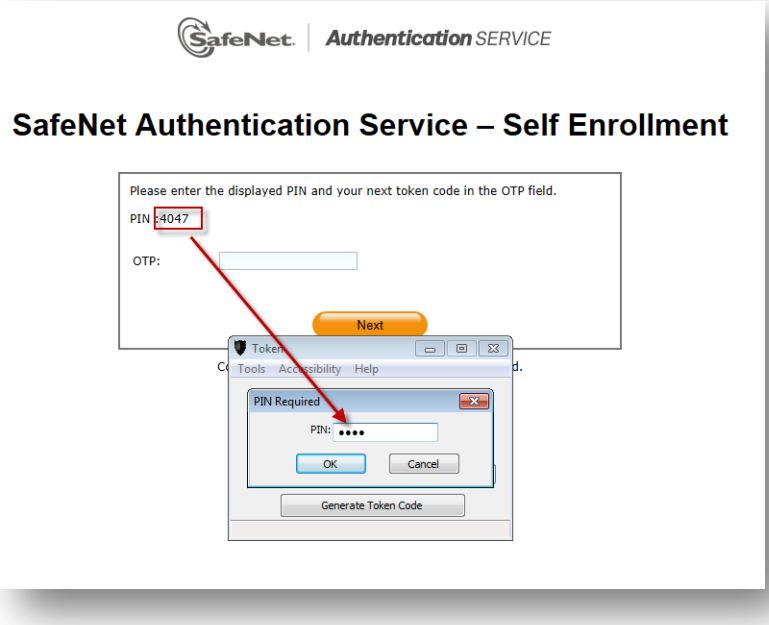
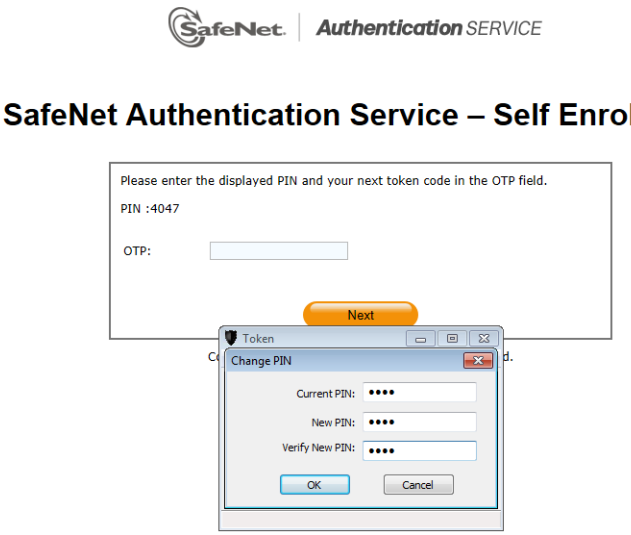


Figure 6: Initial PIN required to Load MP token

Step 5:

Your administrator may require that you change the Initial PIN (Step 4) to a value only you know before the token can generate an OTP. If this is the case, enter the Initial PIN value into the Current PIN field, then enter and verify the new PIN using the remaining fields.



Your token will display an OTP. Enter the token code into the OTP field of the Self-enrollment page., then click “Next” to continue.

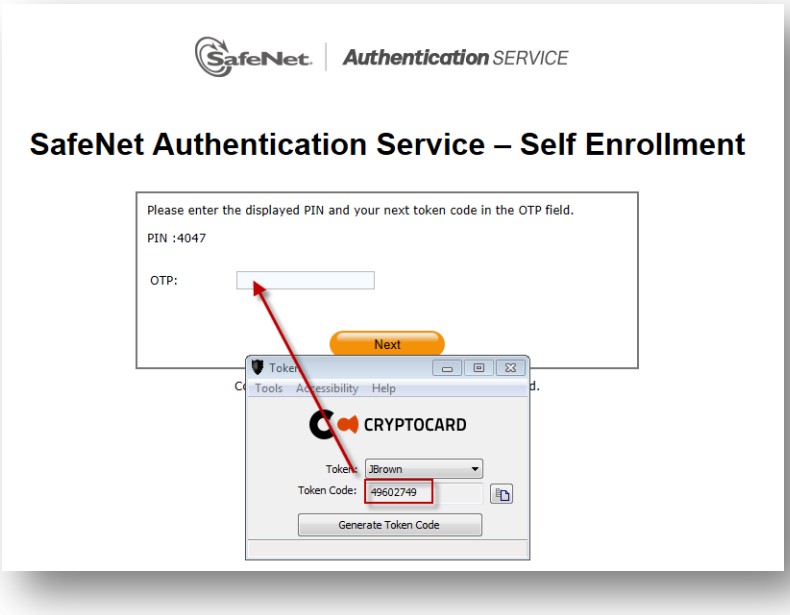


Figure 7: Enter OTP to Complete Enrollment

Your token has been enrolled and can now be used to authenticate.

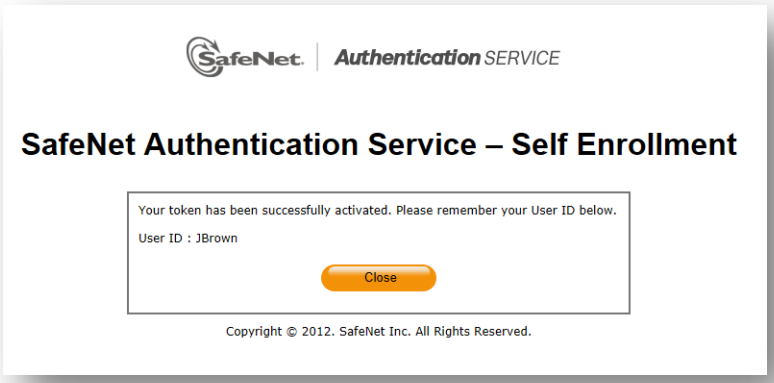


Figure 8: Enrollment Complete Confirmation

How do I use my MP-1

Every time you need an OTP to logon, begin by tapping the MP-1 icon and then enter your Security PIN. If you have more than one token loaded you must select a before you will be prompted to enter your PIN.

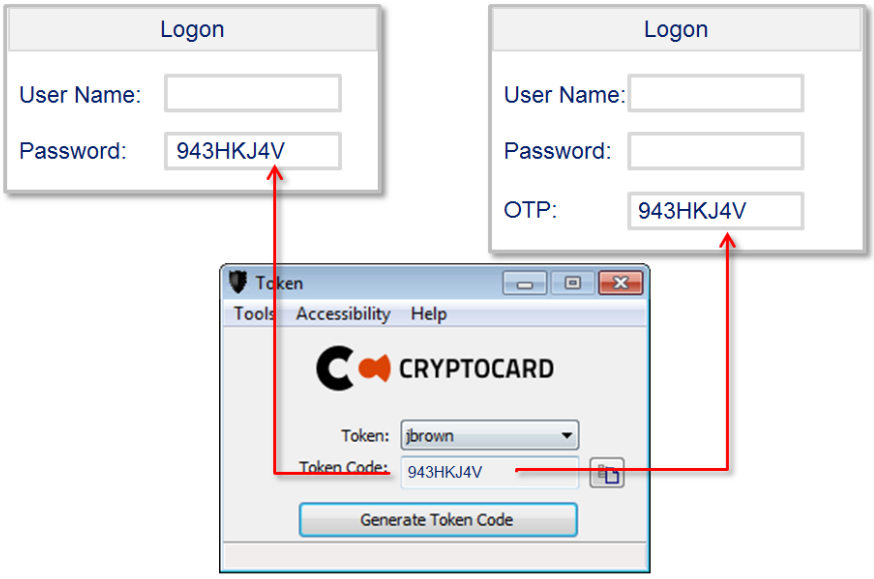


Figure 9: Using the MP-1 OTP

Remember, every time you logon you will enter your Security PIN to generate an OTP, then type or copy the OTP into the appropriate password or OTP field. Use the icon to the right of the Token Code field to copy to clipboard. Right click in the password field to paste the code into the field.

What if my token shuts off while I'm entering the token code?

Simply generate a new token code by clicking the Generate Token Code button and then enter your Security PIN. Enter the Token Code into the appropriate password field and logon as normal.

What are my responsibilities?

Using the MP-1 will not only provide security, it will simplify your life be reducing or eliminating the need to remember or periodically change passwords. Your token will do this for you, every time you logon. However, you do have a few simple obligations:

Protect your Security PIN

Protect your Security PIN just as you would the PIN for your bank or credit card. Never share it with anybody, including people you trust. Your network security administrator and help desk will never ask for your PIN and you should never reveal it to them. Never write down your PIN.

How can I change my PIN?

If you wish to change your PIN or are concerned that it has been compromised tap the "Edit" button (Figure 6: MP-1 with multiple tokens installed on page **Error! Bookmark not defined.**), then tap the blue token tile, then enter your current security PIN. This will display a list of options. Select the "Change PIN" option from the list. Enter and confirm the new security PIN. Tap the "Done" button to exit the edit mode.

What if I forget my PIN?

Contact your help desk. Upon verifying your identity they will be able to reset your PIN.

What if my token is "Locked"

This indicates that there has been an attempt to generate OTPs using an incorrect PIN. Contact your help desk). Upon verifying your identity they will be able to reset your PIN.

What should I do if I can't logon using my token?

The most common cause of failed logon is entering an incorrect OTP. Never attempt to reuse a token code and ensure that you enter the code exactly as displayed on the token, including any upper and lower case letters and punctuation that it may contain.

Your account will automatically lock for a period of time if the maximum number of consecutive failed logon attempts is exceeded. You must wait this amount of time before your account will unlock. Contact the help desk to resolve logon problems.

How long will my token continue to operate?

Your token will be able to generate OTPs until it is revoked by your Security administrator.

Customizing Your Token

You can customize your token in several ways: Change your PIN, Resync the token, Rename the token, generate signatures and unlock a token. To access any of these functions, click the “Tools” option.

Multiple Tokens

It is possible to load several tokens into the MP-1 applications. A dropdown list provides access to additional loaded tokens.

Figure 10: MP with multiple tokens

Change PIN

This option is used to change the PIN of the selected token. You will be required to provide the current PIN and then create and confirm a new PIN.

Resync

This option is rarely required and should only be used on instruction from your help desk. Enter the challenge provided by your administrator (or from the self-service site) and the PIN for the token. Give the resulting token code to your administrator or enter into the appropriate field on the self-service resync page.

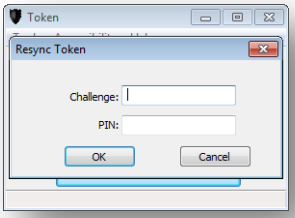


Figure 11: Resync Token – Challenge

Figure 12: Resync Token - Token Code

Unlock Token

If an incorrect PIN is entered into the token too many times consecutively, the token will become locked. If your token is locked, click the Unlock Token option. Contact your administrator if your token is locked and this option is not available.

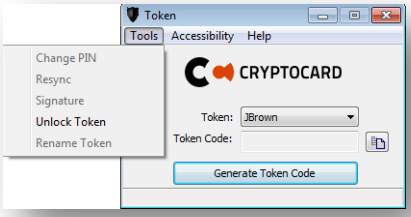
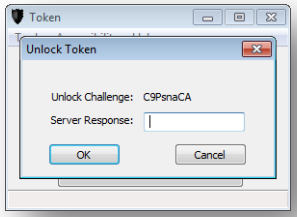


Figure 13: Unlock Token Option



Read the unlock challenge to your administrator exactly as displayed including proper case. Your administrator will provide a “Server Response” which must be entered exactly (case sensitive) as provided, then click OK.

SIGNATURE ON/OFF

The signature function is off by default and should not be used unless advised by your Security administrator.