SafeNet Authentication Manager

Version 8.0 Rev A

User's Guide

Date of publication: September 2010

Last update: Monday, September 20, 2010 3:03 pm

Support

We work closely with our reseller partners to offer the best worldwide technical support services. Your reseller is the first line of support when you have questions about products and services. However, if you require additional assistance you can contact us directly at:

Telephone

You can call our help-desk 24 hours a day, seven days a week:

USA: 1-800-545-6608

International: +1-410-931-7520

Email

You can send a question to the technical support team at the following email address:

support@safenet-inc.com

Website

You can submit a question through the SafeNet Support portal:

http://c3.safenet-inc.com/secure.asp

Additional Documentation

We recommend reading the following SafeNet publications:

- SafeNet Authentication Manager 8.0 Administrator's Guide
- SafeNet Authentication Manager 8.0 ReadMe

Table of Contents

Part I Introduction

1. Token Overview 3
Token Uses 4
Certificate-Based Authentication 4
OTP Generation 4
Secure Data Storage 5
Hardware Tokens 5
Software Tokens 5
SafeNet eToken Virtual Products 5
MobilePASS Tokens 7

2. SafeNet Authentication Manager Overview 9
SafeNet Authentication Manager User Interfaces 10
SafeNet Authentication Manager Tasks 10
Token Management 12
Associating Your Token with SafeNet Authentication Manager 12
Maintaining Your Token 13
Setting Your Token Password or OTP PIN 13
Handling a Forgotten Token Password 14
Handling a Forgotten OTP PIN 14
Preparing to Take Your Token On-the-Road 15
Resolving a Lost Token Locally 15
Resolving a Lost Token On-the-Road 15

Part II Self Service Center

3. Self Service Center 19
Self Service Center Overview 20
Before Any Tokens are Enrolled 20
After Tokens are Enrolled 22

Accessing the Self Service Center Main Menu 25
Installing Software Components for Enrollment 27
Enabling ActiveX Components for Token Enrollment 27
Installing Client Components 30

4. Self Service Center User Activities 41

Enrolling a New Smartcard or USB Token 42
Enrolling a New OTP Token 47
Enrolling a New MobilePASS Token 48
Generating an OTP on Your Mobile Device 50
Enabling a New MobilePASS Messaging Token 51
Enrolling a New SafeNet eToken Virtual 53
Completing Your Authentication Questionnaire 57
Changing Your SafeNet Authentication Manager User Password 59

5. Self Service Center Token Management 61

Updating Your Token Content 62
Changing and Resetting Your Token Password 66
Enabling and Temporarily Disabling Your Token 67
Revoking Your Lost or Damaged Token 69
Replacing or Upgrading Your Token 75
Downloading a SafeNet eToken Rescue 82
Changing and Resetting Your OTP PIN 85
Validating Your OTP Token 86
Enrolling a New SafeNet eToken Virtual Temp 87

6. Self Service Center Rescue Token Management 93

Main Menu 94
Re-enrolling a Lost Token 94
Replacing a Lost Token 98
Downloading a Backup SafeNet eToken Rescue 104

Part III Rescue Service Center

7. Rescue Service Center 107

Rescue Service Center Overview 108
Accessing the Rescue Service Center Main Menu 108

8. Rescue Service Center Token Activities 113

Main Menu 114

Retrieving a Response Code to Unlock Your Token....115
Managing Your Lost or Damaged Token....117
Reporting and Temporarily Replacing Your Lost or Damaged Token 118
Replacing Your Token with a New Token.... 125
Generating an OTP Using Your SafeNet eToken Rescue.... 125
Enabling and Temporarily Disabling Your Token.... 126
Resetting Your OTP PIN.... 127
Validating Your OTP Token.... 128

9. Rescue Service Center Rescue Token Management....131

Main Menu.... 132
Recovering Your SafeNet eToken Rescue Password 133
Replacing Your SafeNet eToken Rescue.... 134
Closing Your SafeNet eToken Rescue.... 137

Part IV SAM Agent

10. SAM Agent 141

SAM Agent Overview 142
Viewing the SAM Agent Status 142
Verifying Your Token Content.... 144
Downloading a SafeNet eToken Rescue 145

Part I Introduction

The following chapters provide an overview of the SafeNet Authentication Manager and the SafeNet tokens that it supports.

In this section:

- Chapter 1: Token Overview (page 3)
- Chapter 2: SafeNet Authentication Manager Overview (page 9)

Chapter 1

Token Overview

This chapter describes various types of tokens and their uses.

In this chapter:

- Token Uses
- Hardware Tokens
- Software Tokens

Token Uses

Tokens, also known as authenticators, are used primarily for some or all of the following purposes:

- Certificate-Based Authentication
- OTP Generation
- Secure Data Storage

Certificate-Based Authentication

A certificate is a signed document approving the identity of the *private key* on a token. The private key acts as a unique identifier for each user. It enables users to securely access networks or protected websites, or to digitally sign data and transactions, providing proof of authenticity.

OTP Generation

One-Time Password (OTP) authentication is based on a system in which the token and the backend authentication service share a unique algorithm used for generating a sequence of passwords. Since the server and the token generate exactly the same passwords in the same sequence, the server can authenticate the user when the token's OTP value is submitted.

OTP authentication enables secure access to networks from any computer with an internet connection. By constantly changing the password required for authentication, OTP usage makes it more difficult to gain unauthorized access to restricted resources.

OTP authentication does not require a physical token to be connected to the computer.

Secure Data Storage

A token may be used for secure storage of data such as:

- User profiles - collections of personal data which identify the user to specific applications
- Flash memory that can be partitioned into a mass storage allocation and a CD-ROM emulation

Hardware Tokens

SafeNet Authentication Manager supports a variety of hardware tokens, including:

- Smartcards
- USB tokens
- OTP tokens

Software Tokens

A software token is a set of one or more files stored on a general-purpose electronic device, such as a computer, portable drive, or mobile phone.

The following software tokens are supported by SafeNet Authentication Manager:

- SafeNet eToken Virtual Products
- MobilePASS Tokens

SafeNet eToken Virtual Products

Depending on the SafeNet eToken Virtual product used, the software authenticator file may be stored on your computer or on a portable drive. The software authenticator is locked to the device and can be used only on the computer or portable drive on which it was enrolled.

When you enroll a SafeNet eToken Virtual or SafeNet eToken Virtual Temp on your computer, or, if the SafeNet Authentication Manager SAM Agent is used to download a SafeNet eToken Rescue, the authenticator is saved in your personal Documents folder, in the `eTokenVirtual` subfolder. Its filename extension is `.etvp`.

Note:
A file copied from a SafeNet eToken Virtual product is not usable.

Your SafeNet Authentication Manager configuration may allow you to enroll the following SafeNet eToken Virtual products:

- **SafeNet eToken Virtual**
  - Can contain the same token content as an eToken NG-OTP device, such as eToken SSO profiles, OTP generation facilities, and certificates
  - Depending on your SafeNet Authentication Manager configuration, can be saved either to your computer, or to a external device
- **SafeNet eToken Virtual Temp**
  - Can contain token content similar to an eToken NG-OTP device, but its certificates are valid only for the time period defined by your administrator
  - One SafeNet eToken Virtual Temp can be enrolled for each physical token already enrolled to you
  - Must be saved to your computer
  - Is usable for a limited period of time
- **SafeNet eToken Rescue**
  - Contains a backup of certain token content, such as Network Logon profiles, OTP generation facilities, and certificates

  Note:
  You may need other token content, such as your WSO profiles, while using your SafeNet eToken Rescue. Restore them to your SafeNet eToken Rescue from backup files.

  - Accessible only through a password that is disclosed when you report your token as lost or damaged
  - Depending on your SafeNet Authentication Manager configuration, can be saved either to your computer, or to a external device

- Depending on your SafeNet Authentication Manager configuration, can be downloaded using the Self Service Center, the Rescue Service Center, or the SAM Agent
- Is usable for a limited period of time

To generate an OTP using a SafeNet eToken Virtual product:

1. If the appropriate SafeNet eToken Virtual authenticator is not connected, browse to its location, right-click the filename, and click **Open** to define the file to *SafeNet Authentication Client*.
2. Right-click the *SafeNet Authentication Client* tray icon, and from the menu, select the appropriate SafeNet eToken Virtual authenticator.
3. Right-click the *SafeNet Authentication Client* tray icon, and from the menu, select **Generate OTP**.

   The *Generate OTP* window opens.
4. Click **Generate OTP**.
5. Depending on your SafeNet Authentication Manager configuration, you may be required to enter the Token Password.

   Enter the SafeNet eToken Virtual product's password.
6. An OTP is generated and displayed.
7. Copy the OTP to your application to authenticate yourself.

MobilePASS Tokens

Your SafeNet Authentication Manager configuration may allow you to enroll a MobilePASS token. A MobilePASS token is an application that can generate an OTP value for authentication.

Install the MobilePASS application on your mobile device to use it as an OTP token that works independently of mobile network connectivity.

Use the MobilePASS Messaging application to receive a generated OTP as an SMS (Short Message Service) message on your mobile device, or as a message sent to your email address.

Chapter 2

SafeNet Authentication Manager Overview

SafeNet Authentication Manager provides a framework of interfaces that enable users to manage their own physical and virtual tokens.

In this chapter:

- SafeNet Authentication Manager User Interfaces
- SafeNet Authentication Manager Tasks
- Token Management

SafeNet Authentication Manager User Interfaces

SafeNet Authentication Manager users may have access to the following features:

- Self Service Center: a web-based service center for managing your tokens from within your company
- Rescue Service Center: a web-based service center for situations in which you are away from your office and are unable to use your token due to a specific problem
- SAM Agent: a SafeNet Authentication Client feature for verifying that your token content and SafeNet eToken Rescue backup file are up-to-date

The user interfaces do not replace the function of your administrator.

SafeNet Authentication Manager Tasks

In your SafeNet Authentication Manager configuration, your administrator has defined which tasks you are authorized to perform.

The following table lists the SafeNet Authentication Manager tasks that can be performed by users, and the features that can be used to perform each one.

Table 2-1. SafeNet Authentication Manager User Tasks

Task	Self Service Center	Rescue Service Center	SAM Agent
Enroll one of the following: ■ Smartcard or USB token ■ OTP token ■ SafeNet eToken Virtual ■ SafeNet eToken Virtual Temp ■ MobilePASS token ■ MobilePASS Messaging token	x		
Check that a token's content is up-to-date	x		x
Update token content	x		
Complete an authentication questionnaire	x		
Change a Token Password or OTP PIN	x		
Reset a Token Password	x		
Retrieve a *Response Code* to unlock a token and reset its Token Password	x In non-Windows environments only	x	
Reset an OTP PIN	x	x	
Upgrade a token by replacing it with a newer model	x		

Table 2-1. SafeNet Authentication Manager User Tasks (Continued)

Task	Self Service Center	Rescue Service Center	SAM Agent
Enable or temporarily disable a token	x	x	
Report and revoke a lost token	x	x	
Replace a lost token with a new token	x		
Replace a lost OTP device with a Temp OTP		x	
Download a SafeNet eToken Rescue	x	x	x
Activate and manage access to a SafeNet eToken Rescue to replace a lost token		x	
Validate an OTP token	x	x	

Token Management

Associating Your Token with SafeNet Authentication Manager

Use the Self Service Center when your administrator tells you to do any of the following:

- Enroll a smartcard or USB token
- Enroll an OTP token
- Enroll a MobilePASS token
- Enroll a MobilePASS Messaging token
- Enroll a SafeNet eToken Virtual

- Enroll a SafeNet eToken Virtual Temp
- Update your token content
- Upgrade your token by replacing it with a more advanced device
- Replace your lost token with a new one

Maintaining Your Token

SafeNet Authentication Manager is designed to help ensure that no one else uses your token. Use a SafeNet Authentication Manager service center to do the following:

- Update your token content if you suspect that content was deleted
- Temporarily disable your token if it is misplaced or if it is not needed for an extended period
- Enable your disabled token when you want to use it again
- Validate your OTP token if your token has lost its synchronization with the system, and you cannot authenticate using a generated OTP
- Change your SafeNet Authentication Manager user password if you suspect that someone else has seen it

Setting Your Token Password or OTP PIN

It is your responsibility to remember your Token Password or OTP PIN. Your SafeNet Authentication Manager configuration may require you to provide it to gain access to your token content.

Change your Token Password or OTP PIN if you suspect it has been compromised.

The default Token Password is 1**234567890**, unless your administrator has changed the default. Your SafeNet Authentication Manager configuration may require you to change your Token Password from the default value.

Depending on your SafeNet Authentication Manager configuration, your Token Password may be required to meet password quality criteria, such as:

- minimum length
- inclusion or exclusion of lower-case letters, upper-case letters, numerals, and/or special characters
- disqualification of password values previously used

Setting a complex Token Password provides added security to your token authentication process.

Handling a Forgotten Token Password

If you forgot your Token Password, or if you consecutively entered incorrect password values too many times, you need to unlock your token and set a new password.

Depending on your SafeNet Authentication Manager configuration, you can use the Self Service Center to reset your Token Password should you forget it.

If your token is locked, and you cannot reset your Token Password, do one of the following:

- In a non-Windows environment, use the Self Service Center to unlock your token.
- Use the Rescue Service Center to enter the **Challenge Code** displayed in the *SafeNet Authentication Client Tools* or *eToken Network Logon* application, and then paste the generated **Response Code** to the application.
- Contact your administrator.

Handling a Forgotten OTP PIN

If you forgot your OTP PIN, or if you consecutively entered incorrect values too many times, you need to unlock your OTP profile and set a new OTP PIN.

Depending on your SafeNet Authentication Manager configuration, you can use the Self Service Center to reset your OTP PIN should you forget it.

If you cannot reset your OTP PIN using the Self Service Center, and your OTP profile is locked, contact your administrator.

Preparing to Take Your Token On-the-Road

Before you travel, use the Self Service Center to do the following:

- Complete an authentication questionnaire to ensure that you will have access to the Rescue Service Center while you are out of the office. The answers you provide will be used to authenticate you to the Rescue Service Center.
- Download a *SafeNet eToken Rescue*, a secure backup of your token content, to ensure that you can request access to a backup of your token content while you are out of the office.

If you already downloaded a SafeNet eToken Rescue, use the SAM Agent to verify that the file is up-to-date.

Resolving a Lost Token Locally

If your token is lost or damaged, do the following:

a. Log on to the Self Service Center, and report your lost or damaged token so that it is revoked.
b. Ask your administrator to give you a new token in its place.
c. Log on to the Self Service Center again, and replace your old token with the new one.

Resolving a Lost Token On-the-Road

If you are away from your office when your token is lost or damaged, use the Rescue Service Center to do the following (depending on the options available in your SafeNet Authentication Manager configuration):

- Report your token as lost or damaged.
- If you will need to authenticate yourself using an OTP but will not need any other token content, request a *Temp OTP* to replace your token.

- If you will need access to your token content and do not have a *SafeNet eToken Rescue* secure backup file, download a *SafeNet eToken Rescue*.
- If you will need access to your token content, activate a downloaded *SafeNet eToken Rescue* to use as a temporary token replacement.
- If you do not need a Temp OTP or a SafeNet eToken Rescue, revoke or temporarily disable your token.

Part II Self Service Center

The following chapters describe how to use SafeNet Authentication Manager's Self Service Center.

In this section:

- Chapter 3: Self Service Center (page 19)
- Chapter 4: Self Service Center User Activities (page 41)
- Chapter 5: Self Service Center Token Management (page 61)

Chapter 3

Self Service Center

SafeNet Authentication Manager's Self Service Center is a web-based application that enables you to manage many user and token activities.

In this chapter:

- Self Service Center Overview
- Accessing the Self Service Center Main Menu
- Installing Software Components for Enrollment

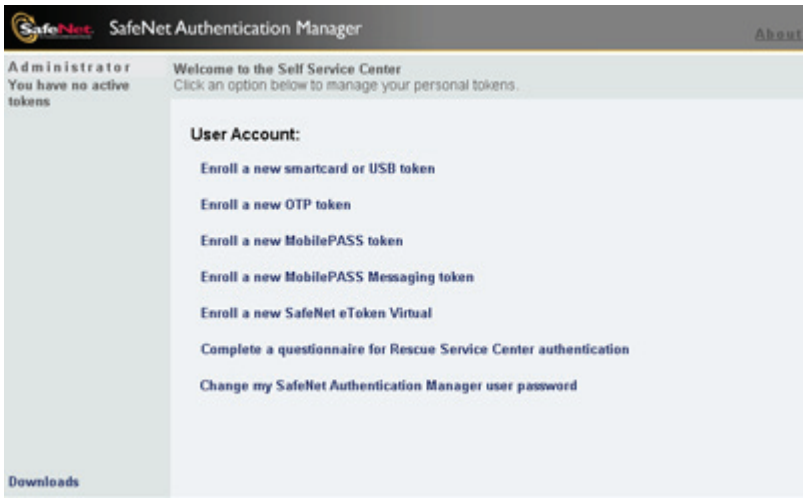
Self Service Center Overview

When you open the SafeNet Authentication Manager's Self Service Center window, a list of your enrolled tokens is displayed in the left panel, and a list of options is displayed in the right panel.

Note:
Your SafeNet Authentication Manager configuration determines which options are displayed in the right panel of the *Welcome to the Self Service Center* window.

Before Any Tokens are Enrolled

The following is an example of a Self Service Center window where no tokens are enrolled.



Left Panel

The following message is displayed in the left panel of the Self Service Center window, below your user name:

You have no active tokens

Right Panel

The right panel may include the following *User Account* options:

- Enrolling a New Smartcard or USB Token

  Token enrollment adds your smartcard or USB token to the SafeNet Authentication Manager inventory if it is not already there, associates the token with your username, and loads its content with the data you need.

- Enrolling a New OTP Token

  OTP (One-Time Password) token enrollment associates your physical OTP token, which is not a smartcard or a USB token, with your username in the SafeNet Authentication Manager inventory.

- Enrolling a New MobilePASS Token

  MobilePASS token enrollment installs a MobilePASS application on your mobile device, enabling you to generate an OTP on the device.

- Enabling a New MobilePASS Messaging Token

  MobilePASS Messaging token enrollment enables you to receive a generated OTP as an email message, or as an SMS (Short Message Service) message on your mobile device.

- Enrolling a New SafeNet eToken Virtual

  SafeNet eToken Virtual enrollment enrolls a software token. Depending on your SafeNet Authentication Manager configuration, a SafeNet eToken Virtual is stored as a file on your computer, or on a portable drive.

- Completing Your Authentication Questionnaire

  Before you can authenticate yourself to the Rescue Service Center, you must complete an authentication questionnaire in the Self Service Center. This provides a backup method of identifying yourself in case you lose your token or forget its password when you are out of the office.

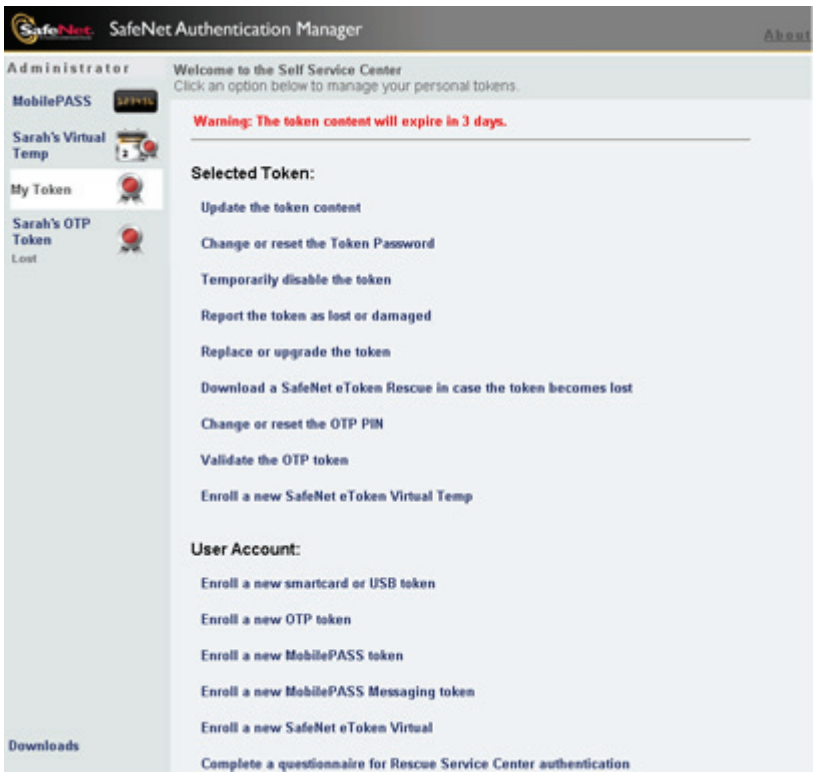
- Changing Your SafeNet Authentication Manager User Password

  Users in some SafeNet Authentication Manager environments authenticate to SafeNet Authentication Manager using a user password. Change your user password if you think someone else has seen it.

Note:
Your SafeNet Authentication Manager configuration determines which options are displayed in the right panel.

After Tokens are Enrolled

The following is an example of a Self Service Center window where at least one token is enrolled.



Left Panel

A list of the names of your enrolled tokens is displayed in the left panel of the Self Service Center window, below your user name. An image representing the token type is displayed next to each token name. If the token's status is not *Normal*, the status is displayed:

- Lost
- Damaged
- Disabled
- Revoked

The selected token is highlighted. If you need to perform an action on a different token, select the appropriate token in the left panel before selecting an option in the right panel.

Right Panel

The right panel includes messages relating to the selected token, followed by *User Account* options. For the list of *User Account* options, see page 21.

The *Selected Token* options displayed in the right panel may include:

- Updating Your Token Content

  If you accidentally deleted content from your token, or if a warning message is displayed that your token content must be updated, use this option to update it.

- Changing and Resetting Your Token Password

  Change your password if it is about to expire, or if you think someone else has seen it.

  Depending on your SafeNet Authentication Manager configuration, you may be able to reset your password should you forget it.

- Enabling and Temporarily Disabling Your Token

  Temporarily disable your token if it is misplaced, or if it is not needed for an extended period.

  If your token is disabled, you must enable it before you can use it again.

- Revoking Your Lost or Damaged Token

  Revoke a lost or damaged token immediately to prevent anyone else from using its content.

- Replacing or Upgrading Your Token

  Revoke your token, and load a new one with the same content.

- Downloading a SafeNet eToken Rescue

  Prepare a backup of your token content in case you lose your token when you are away from your office and cannot replace it with a new one.

- Changing and Resetting Your OTP PIN

  Change your OTP PIN if you think someone else has seen it.

  Depending on your SafeNet Authentication Manager configuration, you may be able to reset your OTP PIN should you forget it.

- Validating Your OTP Token

  If you repeatedly generate an OTP without submitting one for authentication, or if the time function of your OTP token has deviated, your OTP token loses its synchronization with the system. You must validate your OTP token so that SafeNet Authentication Manager can authenticate OTPs that are subsequently generated.

- Enrolling a New SafeNet eToken Virtual Temp

  SafeNet eToken Virtual Temp enrollment creates a software token on your computer that can be used for a limited period of time in place of a token that has been enrolled. The SafeNet eToken Virtual Temp is loaded with token content similar to the content loaded on your enrolled physical token.

Note:
Your SafeNet Authentication Manager configuration determines which options are displayed in the right panel.

Accessing the Self Service Center Main Menu

To access the Self Service Center, you must be logged on to your company's local network.

Access to the Self Service Center requires one of the following authentication methods:

- The standard Windows user authentication method
- The authentication method set by your administrator

Note:
Each company has its own SafeNet Authentication Manager server. This guide uses the name **localhost** to represent your company's SafeNet Authentication Manager server. When following the steps in the procedure, replace **<localhost>** with the name of your company's SafeNet Authentication Manager server.

To access the Self Service Center main menu:

1. Open your web browser, and go to http://<localhost>/SAMservice where **<localhost>** is the name of your company's SafeNet Authentication Manager server.

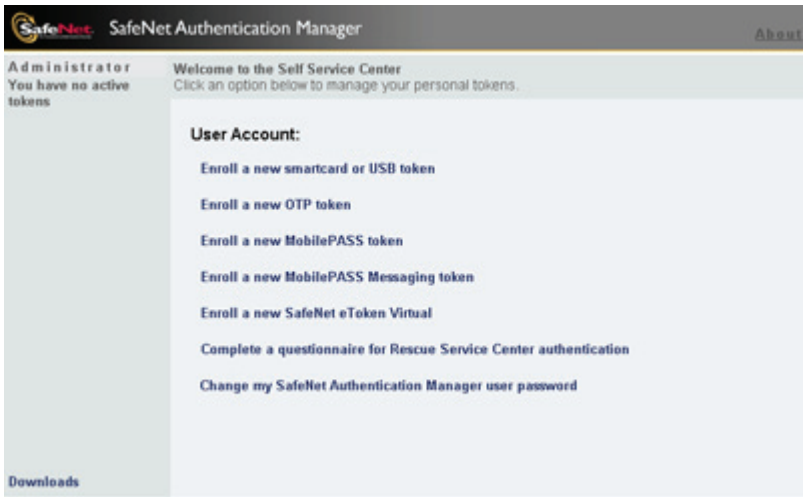
   Note:
   For the website to display properly, ensure that the browser's *Text Size* is set to *Medium*.
   a. On the browser toolbar, click **View**.
   b. From the dropdown menu, select **Text Size** > **Medium**.

   ---

2. Depending on your user store, the *Self Service Center Logon* window may open.

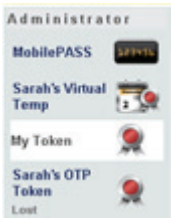
- You may be required to provide logon credentials, such as your *Domain*, *User Name*, and *Password*.
- You may have an option to select **Keep me signed in**, which enables you to re-open the Self Service Center within a predefined time period without logging on again.

3. The *Welcome to the Self Service Center* window opens.



- If you have no enrolled tokens, the following message is displayed in the left panel of the Self Service Center window:
  You have no active tokens

- If you have at least one enrolled token, a list of your tokens is displayed in the left panel of the Self Service Center window, below your user name. The list includes the names of each of your tokens, their representative token images, and their status if not *Normal*.



The selected token is highlighted.

Note:
For more information, see *Self Service Center Overview* on page 20.

4. Select a *User Account* option in the right panel, or select a token in the left panel and select from its *Selected Token* options.
5. To exit the Self Service Center, close the browser.

Installing Software Components for Enrollment

The token enrollment process requires that the following software components be installed on your computer:

- Security settings that enable ActiveX components
- SafeNet Authentication Client
- SafeNet Authentication Manager Client

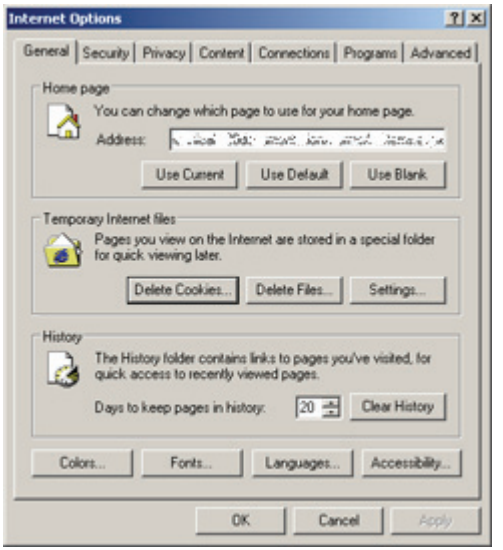
Depending on your SafeNet Authentication Manager configuration, you may be authorized to install some or all of these components without the assistance of your administrator.

Enabling ActiveX Components for Token Enrollment

Before enrolling a token, ensure that the browser's security settings are configured to include the SafeNet Authentication Manager service center in your computer's *trusted sites* zone.

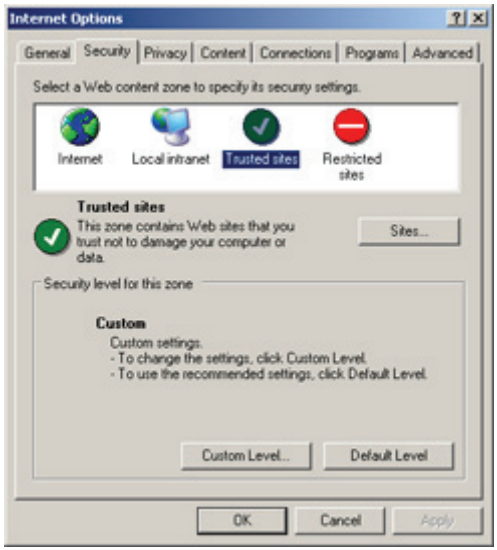
To include the SafeNet Authentication Manager service center in your computer's *trusted sites* zone:

1. On your computer, open the *Internet Explorer* browser.
2. On the toolbar, click **Tools**, and from the dropdown menu, select **Internet Options**.
   The *Internet Options* window opens.



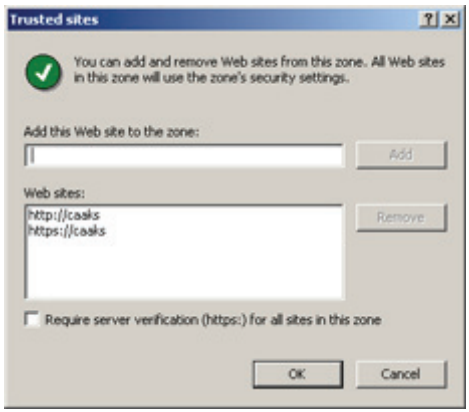
3. Select the **Security** tab.

The *Security* tab opens.



4. In the *Web content zone* box, select **Trusted sites**.
5. Click **Sites**.

   The *Trusted sites* window opens.



6. In the *Add this website* field, enter the URL of the SafeNet Authentication Manager service center.
7. If the SafeNet Authentication Manager service center website URL begins with *HTTPS*, select **Require server verification (https:) for all sites in the zone**. Otherwise, clear this option.
8. Click **OK** until all windows are closed.

9. If your browser's security settings are still not configured to enable ActiveX components for token enrollment, contact your administrator.

Installing Client Components

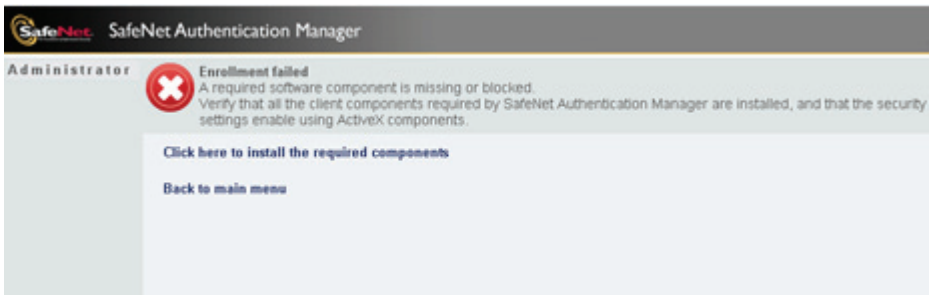
Two client components must be installed on all client computers used for enrolling USB tokens, smartcards, or SafeNet eToken Virtual products:

- SafeNet Authentication Manager Client
- SafeNet Authentication Client

To install a client component on your computer:

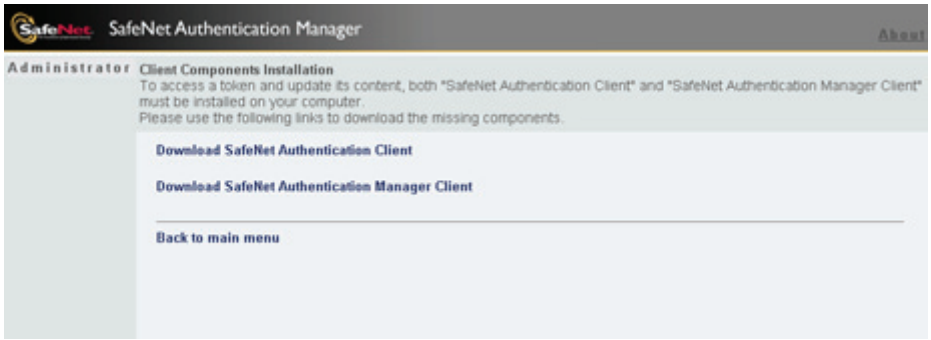
1. Connect a token to be enrolled.
2. In the *Welcome to the Self Service Center* window, select an option to enroll a USB token, smartcard, or SafeNet eToken Virtual product.

   If *SafeNet Authentication Client* or *SafeNet Authentication Manager Client* is not installed on your computer, the *Enrollment failed* window opens.



3. Click the link **Click here to install the required components**.

The *Client Components Installation* window opens.



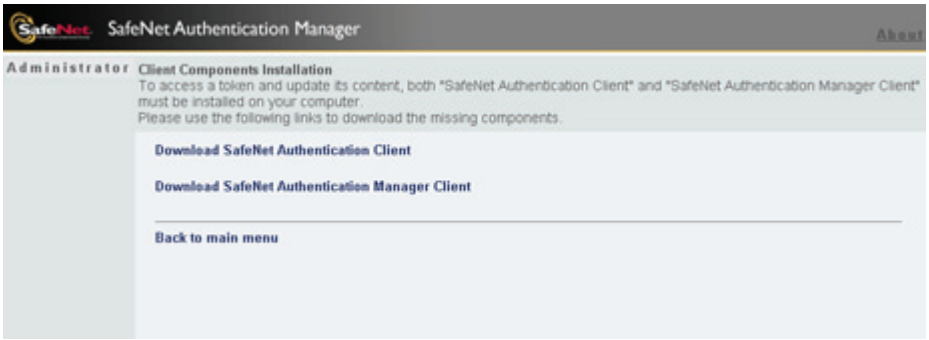
4. Click the appropriate link to download the missing component.
   - To install SafeNet Authentication Client, see *Installing SafeNet Authentication Client* on page 31.
   - To install SafeNet Authentication Manager Client, see *Installing SafeNet Authentication Manager Client* on page 35.
5. When the missing components have been installed, close the browser window, and reopen the Self Service Center.

Installing SafeNet Authentication Client

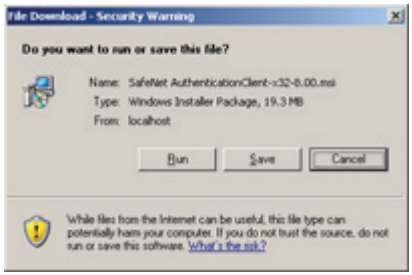
To install SafeNet Authentication Client on your computer:

1. Open the *Client Components Installation* window.
   For more information, see *Installing Client Components* on page 30.

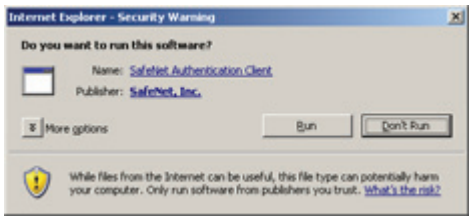
   Note:
   Contact your administrator if SafeNet Authentication Client is not installed and the SafeNet Authentication Client download link is not displayed.



2. Click the link **Download SafeNet Authentication Client**.
   The *File Download* window opens.



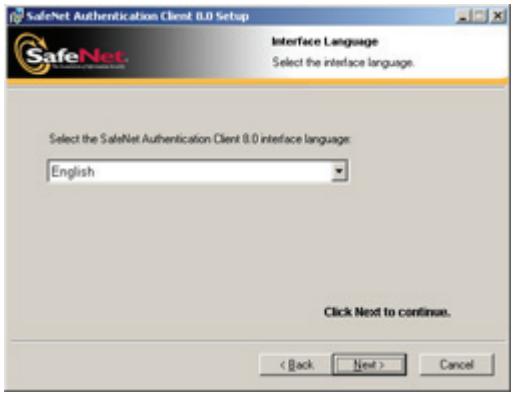
3. Click **Run**.
   A *Security Warning* window opens, identifying the name of the program.



4. Click **Run**.
   Depending on your SafeNet Authentication Manager configuration, an installation wizard may be initiated to install SafeNet Authentication Client.

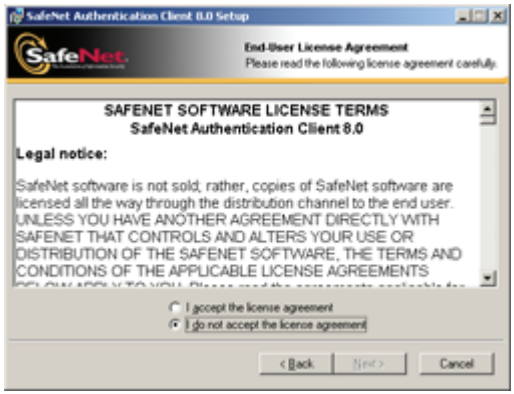
The *SafeNet Authentication Client Installation Wizard* opens.

5. Click **Next**.
   The *Interface Language* window opens.



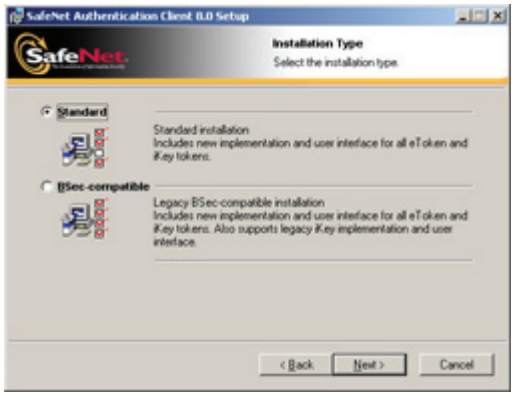
6. From the dropdown list, select the language in which the SafeNet Authentication Manager screens will appear.
7. If configuration settings are detected from a previous version, you can select **Use the existing configuration settings**.
8. Click **Next**.

The *End-User License Agreement* is displayed.



9. Read the license agreement, and select the option, **I accept the license agreement**.
10. Click **Next**.

    The *Installation Type* window opens.

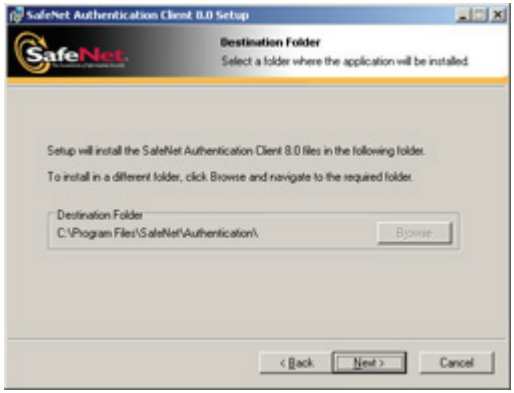


11. Select **Standard**.

Note:
If your administrator has instructed you to run the legacy BSec-compatible installation, select **BSec-compatible.**

12. Click **Next**.

The *Destination Folder* window opens, displaying the default installation folder.



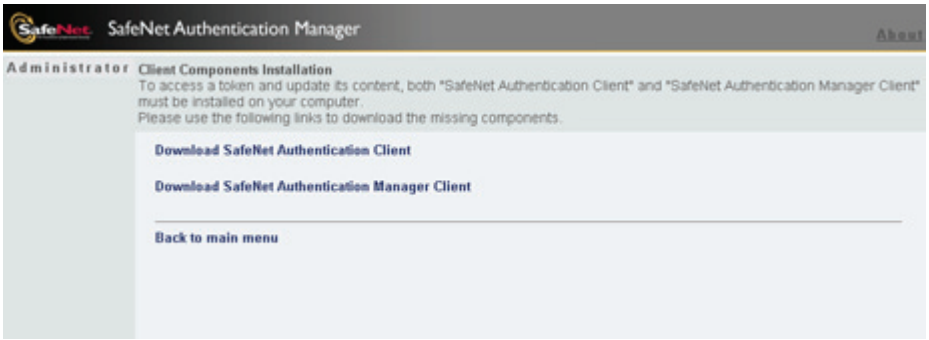
13. Click **Next** to begin the installation.
    When the installation is complete, the *Successfully installed* message is displayed.

14. Click **Finish**.

Installing SafeNet Authentication Manager Client

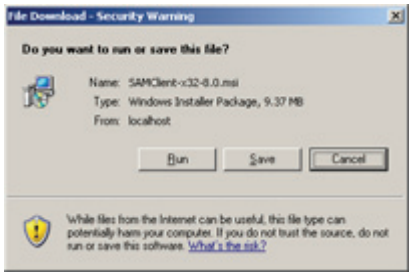
To install SafeNet Authentication Manager Client on your computer:

1. Open the *Client Components Installation* window.
   For more information, see *Installing Client Components* on page 30.



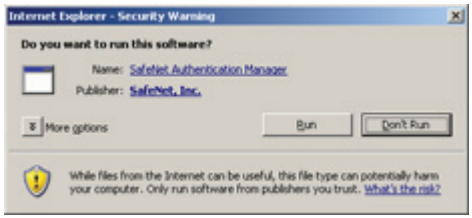
2. Click the link **Download SafeNet Authentication Manager Client**.

   The *File Download* window opens.



3. Click **Run**.

   A *Security Warning* window opens, identifying the name of the program.



4. Click **Run**.

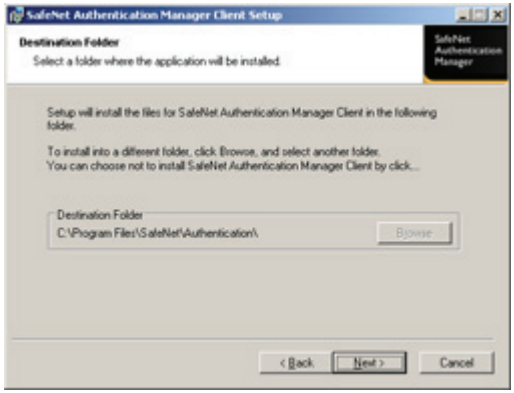
   Depending on your SafeNet Authentication Manager configuration, an installation wizard may be initiated to install SafeNet Authentication Manager Client.

The *SafeNet Authentication Manager Client Installation Wizard* opens.

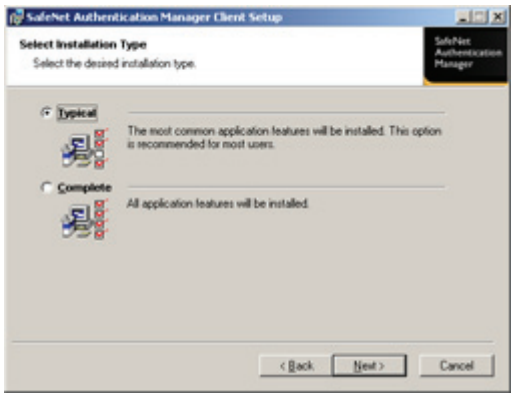
5. Click **Next**.
   The *End-User License Agreement* is displayed.

6. Read the license agreement, and select the option, **I accept the license agreement**.
7. Click **Next**.

The *Destination Folder* window opens, displaying the default installation folder.



8. Click **Next**.
   The *Select Installation Type* window opens.



9. Depending on your SafeNet Authentication Manager configuration, you may be required to select the installation type.
   Select **Typical.**

Note:
If your administrator has instructed you to install the legacy *Desktop Agent*, select **Complete.**

---

10. Click **Next** to begin the installation.

When the installation is complete, the *Successfully installed* message is displayed.

11. Click **Finish**.

Self Service Center User Activities

Use SafeNet Authentication Manager's Self Service Center to manage user activities.

In this chapter:

- Enrolling a New Smartcard or USB Token
- Enrolling a New OTP Token
- Enrolling a New MobilePASS Token
- Enabling a New MobilePASS Messaging Token
- Enrolling a New SafeNet eToken Virtual
- Completing Your Authentication Questionnaire
- Changing Your SafeNet Authentication Manager User Password

Enrolling a New Smartcard or USB Token

Your administrator may ask you to enroll your new smartcard or USB token yourself.

When you enroll a token, the following steps take place:

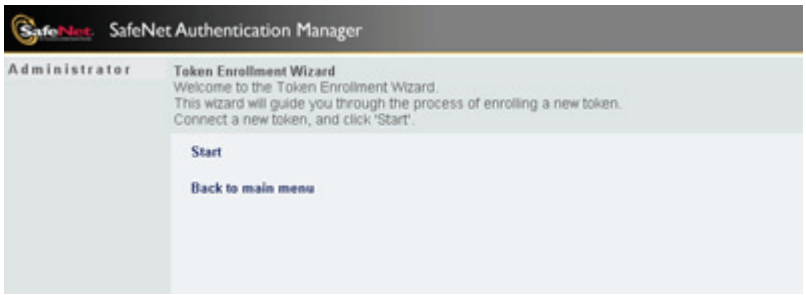
a. The token is added to the SafeNet Authentication Manager inventory if it is not already there.
b. The token is associated with your username.
c. The token is loaded with the data you need.

To enroll a new smartcard or USB token:

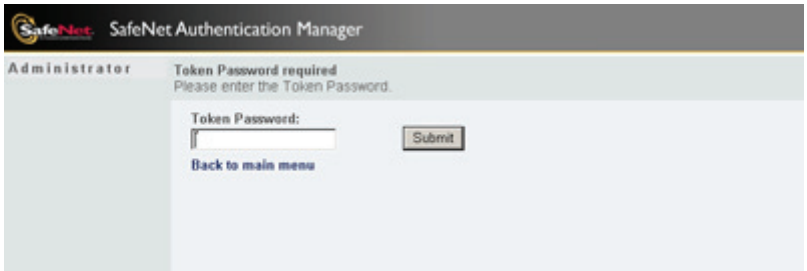
1. In the *Welcome to the Self Service Center* window, select **Enroll a new smartcard or USB token**.

   Note:
   If a required software component is not installed on your computer, the *Enrollment failed* window opens during the attempted enrollment. For more information, see Chapter 3, *Installing Software Components for Enrollment*, on page 27.

   The *Token Enrollment Wizard* opens.



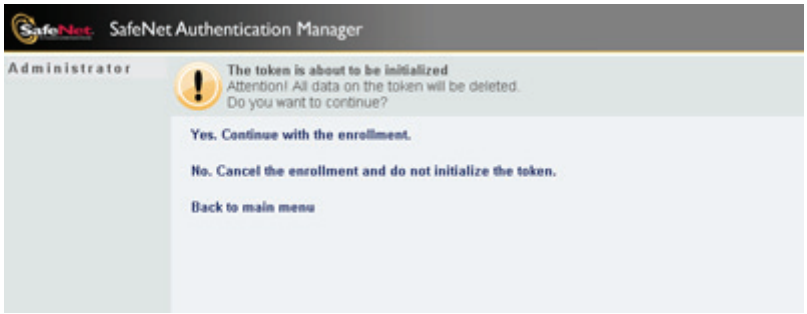
2. Connect the token to be enrolled, and click **Start**.
3. Depending on your SafeNet Authentication Manager configuration, you may be required to enter the Token Password.



Enter the default Token Password used in your company, and click **Submit**.

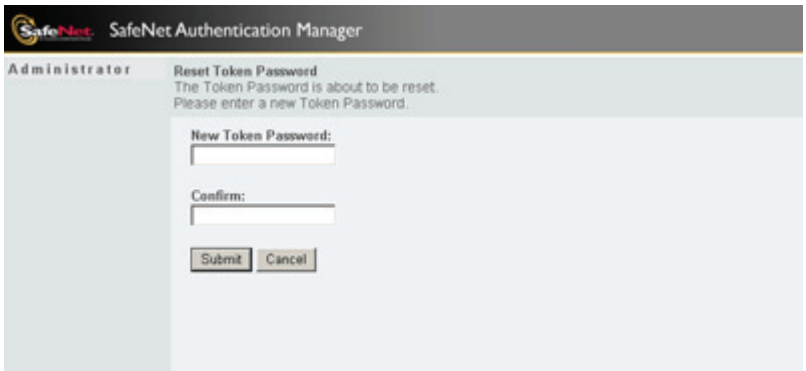
Note:
The default Token Password is **1234567890**, unless your administrator has changed the default.

4. Depending on your SafeNet Authentication Manager configuration, a warning may be displayed that the token is about to be initialized.



Select **Yes. Continue with enrollment**.

5. Depending on your SafeNet Authentication Manager configuration, you may be required to set a new Token Password.



Enter a Token Password that is different from the token's previous Token Passwords, confirm it, and click **Submit**.

Tip:
It is your responsibility to remember your new Token Password. You must provide it to authenticate yourself when you access your token content.

Note:
Depending on your SafeNet Authentication Manager configuration, your Token Password may be required to comply with password quality settings, such as:

- minimum length
- inclusion or exclusion of lower-case letters, upper-case letters, numerals, and/or special characters
- disqualification of password values previously used

6. The *Set Token Name* window opens, displaying the default token name defined in your SafeNet Authentication Manager configuration.

7. You may change the token name. In this example, the token name is changed to **Sarah's OTP Token**.

Tip:
If you have more than one token, we recommend assigning each one a unique token name.

8. Click **Submit**.
9. Depending on your SafeNet Authentication Manager configuration, you may need to do any of the following:
   - Enter a certificate password.
   - If you are enrolling an OTP token, set a new OTP PIN.
   - Enter and confirm your user password.

Click **Submit**.

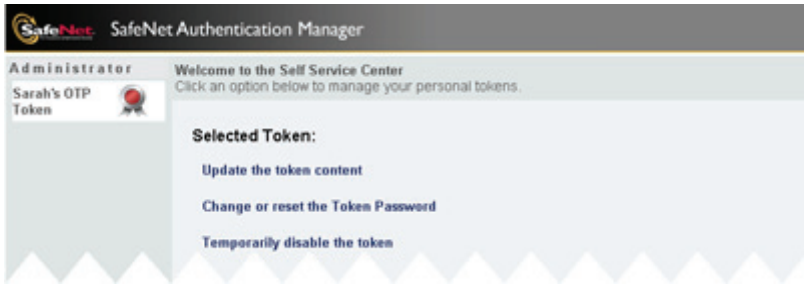
Tip:
It is your responsibility to remember your new OTP PIN. You must provide it to authenticate yourself when you use your OTP.

10. When the enrollment is completed, the following information is displayed:
    - an *Enrollment successfully completed* message
    - the token name
    - other details

Note:
If the details displayed are incorrect, you can change them by updating the token content. For more information, see *Updating Your Token Content* on page 62.

11. Click **Back to main menu** to return to the *Welcome to the Self Service Center* window.

    The name of the enrolled token is displayed in the left panel.



12. Select an option from the right panel, or close the browser to exit the Self Service Center.

Enrolling a New OTP Token

Physical tokens that are not smartcards or USB-compatible tokens can be used to generate an OTP (One-Time Password) for authentication to your application.

Your administrator may have enrolled your new OTP token before giving it to you, or you may be asked to enroll it yourself.

OTP token enrollment associates your OTP device with your username in the SafeNet Authentication Manager inventory.

To enroll a new non-USB OTP token:

1. Have your OTP device in front of you so that you can identify the serial number printed on the label of the OTP device case.

   If the printed serial number is not readable, contact your administrator.
2. In the *Welcome to the Self Service Center* window, select **Enroll a new OTP token.**

The *OTP Token Enrollment* window opens.

3. In the **OTP Token Serial Number** field, enter the serial number printed on the label of your OTP device case.
4. Depending on your SafeNet Authentication Manager configuration, you may be required to set a new OTP PIN, and confirm it.

Tip:
It is your responsibility to remember your new OTP PIN. You must provide it to authenticate yourself when you use your OTP.

5. Click **Submit**.

   The enrollment process begins.
6. Your OTP token is enrolled in SafeNet Authentication Manager, and a *Process successfully completed* message is displayed.
7. Click **Back to main menu** to return to the *Welcome to the Self Service Center* window.

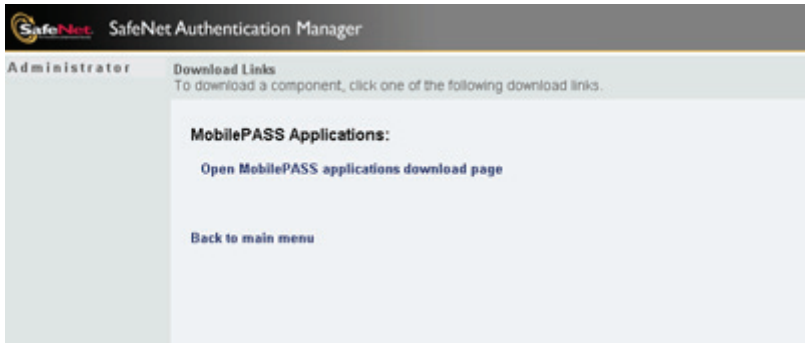
Enrolling a New MobilePASS Token

Enroll a MobilePASS token to generate an OTP on your mobile device without the need for a physical token. The token works independently of mobile network connectivity.

To enroll a new MobilePASS token for your mobile device:

1. At the bottom of the left panel in the *Welcome to the Self Service Center* window, click **Downloads**.

   The *Download Links* window opens.



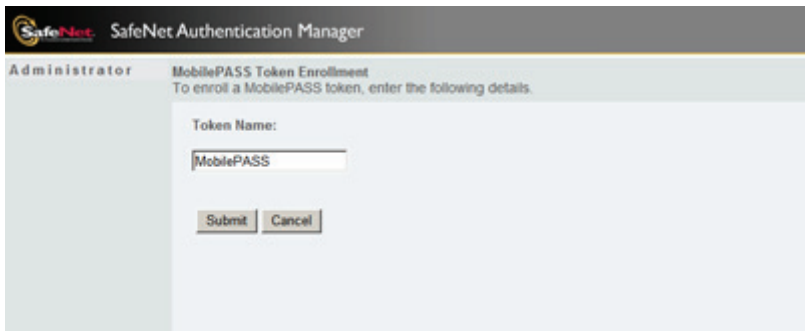
2. Click **Open MobilePASS applications download page**.

   The SafeNet website opens to the *MobilePASS Authenticators Download Page*. Use the link on the SafeNet website to download the appropriate MobilePASS application for your mobile device.

   An Activation Code is displayed on your mobile device. You will need this Activation Code in step 7.

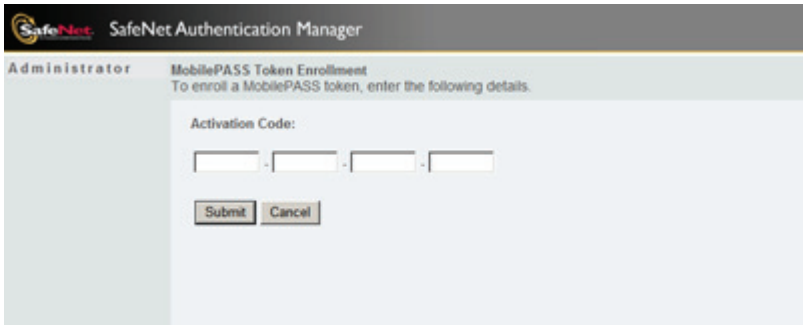
3. In the *Download Links* window, click **Back to main menu**.
4. In the *Welcome to the Self Service Center* window, select **Enroll a new MobilePASS token**.

   The *Token Name* window opens, displaying the default MobilePASS token name defined in your SafeNet Authentication Manager configuration.

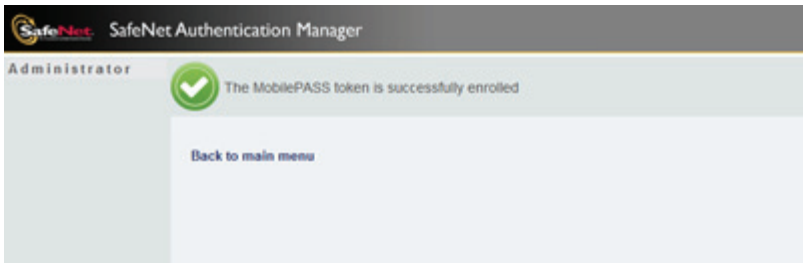


5. You may change the token name.
6. Click **Submit**.

The *Activation Code* window opens.



7. Enter the Activation Code that was displayed on your mobile device in step 2, and click **Submit**.
   The *MobilePASS token successfully enrolled* window opens.



8. Click **Back to main menu** to return to the *Welcome to the Self Service Center* window.

Generating an OTP on Your Mobile Device

After the MobilePASS application is installed, use your mobile device to generate an OTP.

To generate an OTP on your mobile device:

1. On your mobile device select the MobilePASS application.
   A prompt may be displayed requesting your **MobilePASS PIN**.
2. Enter your **MobilePASS PIN**.
3. Generate an OTP.
   The generated OTP is displayed for a limited period of time.
4. Use the generated OTP to authenticate to your application.

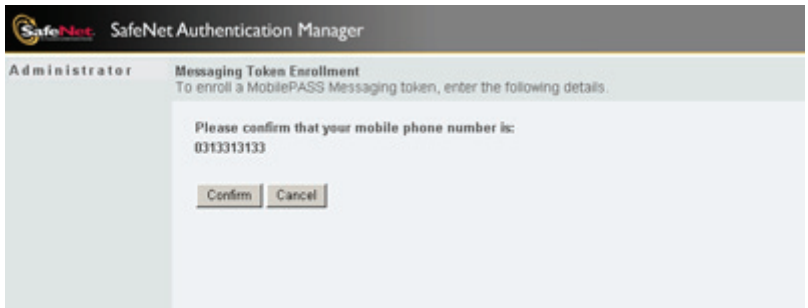
Enabling a New MobilePASS Messaging Token

Enroll a MobilePASS Messaging token to enable the system to send generated OTP passcodes on demand to your mobile device or email address.

To enroll a new MobilePASS Messaging token:

1. In the *Welcome to the Self Service Center* window, select **Enroll a new MobilePASS Messaging token**.

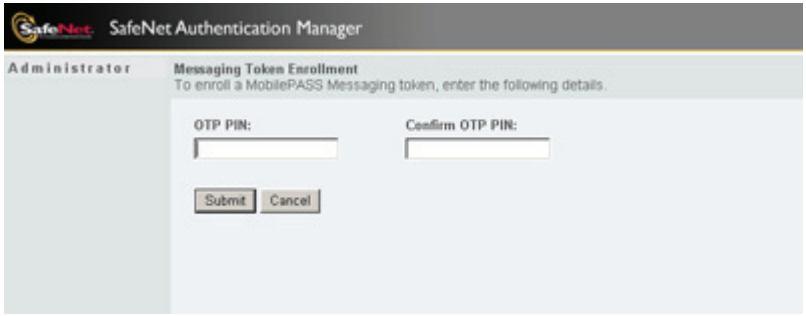
   The *Messaging Token Enrollment* window opens, displaying the mobile phone number or email address that is defined in your SafeNet Authentication Manager configuration.



2. Do one of the following:
   - If the information displayed is incorrect, click **Cancel**, and contact your administrator.
   - If the information displayed is correct, click **Confirm**.

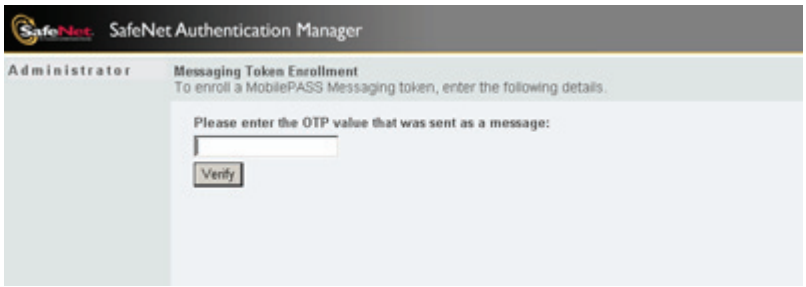
     An OTP passcode value is sent as a message to the mobile phone number or email address displayed in the window. You will need this OTP passcode in step 5.

3. Depending on your SafeNet Authentication Manager configuration, you may be required to set a new OTP PIN.



Enter an OTP PIN, confirm it, and click **Submit**.

4. The *Please enter the OTP* window opens.

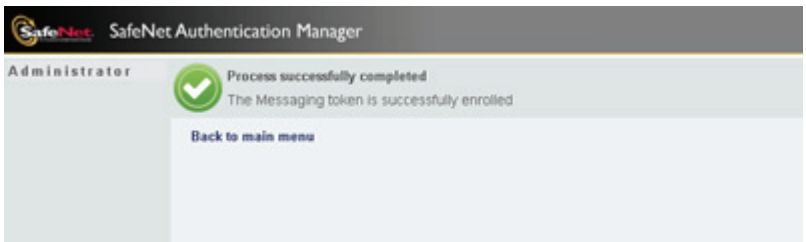


5. Enter the OTP passcode value you received in step 2.

   Depending on your SafeNet Authentication Manager configuration, you may be required to enter the OTP value preceded or followed by your OTP PIN or Windows password.

6. Click **Verify**.

   The *Messaging token successfully enrolled* window opens.



7. Click **Back to main menu** to return to the *Welcome to the Self Service Center* window.

Enrolling a New SafeNet eToken Virtual

SafeNet eToken Virtual enrollment creates a software token on your computer or portable drive.

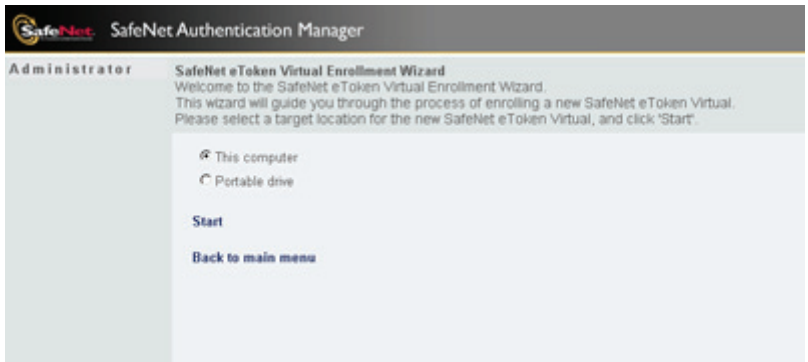
For more information, see Chapter 1, *SafeNet eToken Virtual Products*, on page 5.

To enroll a new SafeNet eToken Virtual:

1. Disconnect all tokens.
2. In the *Welcome to the Self Service Center* window, select **Enroll a new SafeNet eToken Virtual**.

Note:
If a required software component is not installed on your computer, the *Enrollment failed* window opens during the attempted enrollment. For more information, see Chapter 3, *Installing Software Components for Enrollment*, on page 27.

The *SafeNet eToken Virtual Enrollment Wizard* opens.

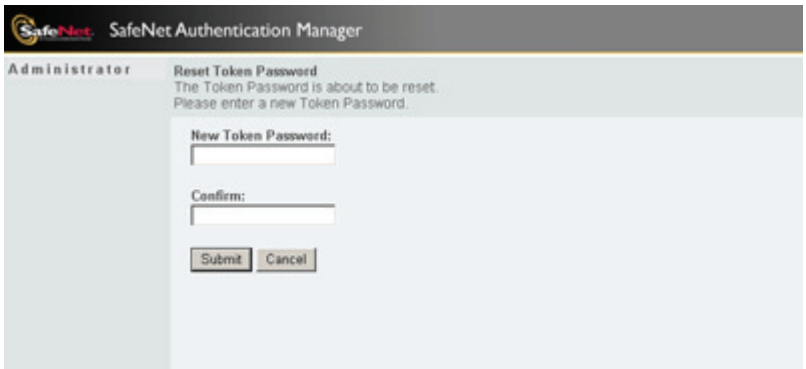


3. Depending on your SafeNet Authentication Manager configuration, you may be required to select the location of the new SafeNet eToken Virtual:
   - **This computer**
   - **Portable drive**

Note:
The portable drive must be connected.

---

4. Click **Start**.
5. Depending on your SafeNet Authentication Manager configuration, you may be required to set a new Token Password.



Enter a new Token Password, confirm it, and click **Submit**.

Tip:
It is your responsibility to remember your new Token Password. You must provide it to authenticate yourself when you access your token content.

Note:
Depending on your SafeNet Authentication Manager configuration, your Token Password may be required to comply with password quality settings, such as:

- minimum length
- inclusion or exclusion of lower-case letters, upper-case letters, numerals, and/or special characters
- disqualification of password values previously used

6. The *Set Token Name* window opens.

7. You may change the SafeNet eToken Virtual name.
   In this example, the token name is changed to **Sarah's Virtual Token**.

Tip:
If you have more than one token, we recommend assigning each one a unique token name.

8. Click **Submit**.
9. Depending on your SafeNet Authentication Manager configuration, you may need to do any of the following:
   - Enter a certificate password.
   - If you are enrolling an OTP token, set a new OTP PIN.
   - Enter and confirm your user password.

Click **Submit**.

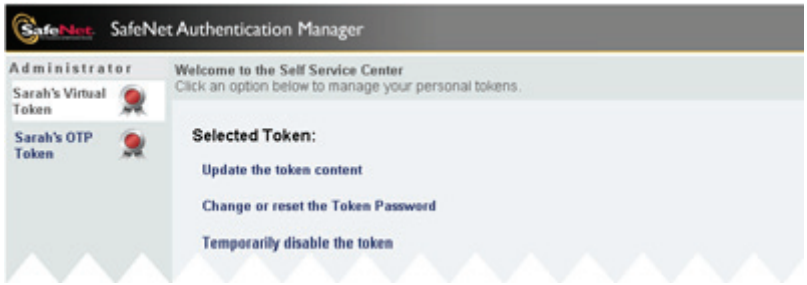
Tip:
It is your responsibility to remember your new OTP PIN. You must provide it to authenticate yourself when you use your OTP.

10. When the enrollment is completed, the following information is displayed:
    - an *Enrollment successfully completed* message
    - the token name
    - other details

Note:
If the details displayed are incorrect, you can change them by updating the token content. For more information, see *Updating Your Token Content* on page 62.

11. Click **Back to main menu** to return to the *Welcome to the Self Service Center* window.

    The name of the enrolled token is displayed in the left panel.



12. Select an option from the right panel, or close the browser to exit the Self Service Center.

Completing Your Authentication Questionnaire

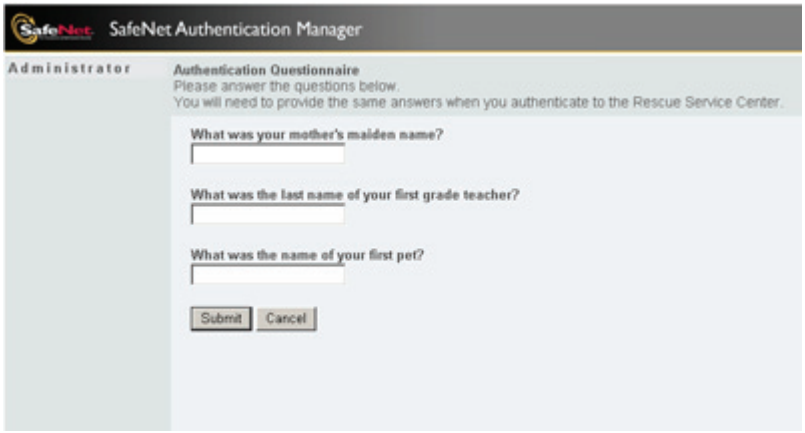
To identify yourself when you are on-the-road and cannot use your token, your administrator may have prepared an authentication questionnaire for you to complete. Your answers are used as a way to identify yourself to the Rescue Service Center, and to other management functions.

The Rescue Service Center provides a solution for situations in which you are out of the office and cannot contact your administrator for help. For more information, see *Rescue Service Center* on page 105.

To complete the authentication questionnaire:

1. In the *Welcome to the Self Service Center* window, select **Complete a questionnaire for Rescue Service Center authentication.**

   The *Authentication Questionnaire* window opens, displaying authentication questions.



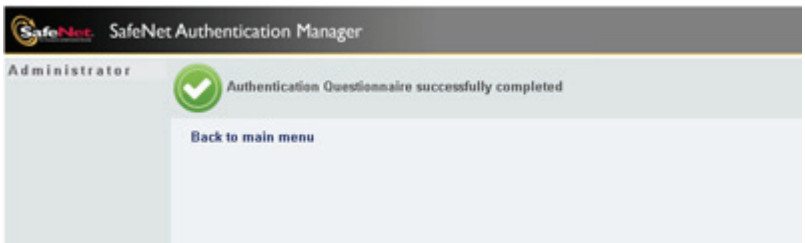
Note:
Each company defines its own authentication questions. The questionnaire shown is an example.

2. Answer the questions.

Note:
When authenticating to the Rescue Service Center, you must provide the same answers you entered in this questionnaire. Questionnaire answers are not case-sensitive.

3. Click **Submit**.

   An *Authentication Questionnaire successfully completed* message is displayed.



4. Click **Back to main menu** to return to the *Welcome to the Self Service Center* window.

Changing Your SafeNet Authentication Manager User Password

Depending on your SafeNet Authentication Manager configuration, you may be assigned a SafeNet Authentication Manager user password.

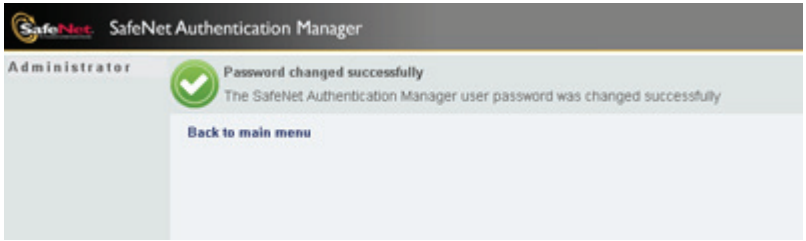
To change your SafeNet Authentication Manager user password:

1. In the *Welcome to the Self Service Center* window, select **Change my SafeNet Authentication Manager user password**.
   The *Change user password* window opens.

2. Do the following:
   a. Enter your current SafeNet Authentication Manager user password.
   b. Enter a new SafeNet Authentication Manager user password, and confirm it.
   c. Click **Submit**.

Tip:
It is your responsibility to remember your new SafeNet Authentication Manager user password. You must provide it to authenticate yourself to SafeNet Authentication Manager.

Your SafeNet Authentication Manager user password is changed, and the *Password changed successfully* message is displayed.



3. Click **Back to main menu** to return to the *Welcome to the Self Service Center* window.

Chapter 5

Self Service Center Token Management

Use SafeNet Authentication Manager's Self Service Center to manage token activities.

In this chapter:

- Updating Your Token Content
- Changing and Resetting Your Token Password
- Enabling and Temporarily Disabling Your Token
- Revoking Your Lost or Damaged Token
- Replacing or Upgrading Your Token
- Downloading a SafeNet eToken Rescue
- Changing and Resetting Your OTP PIN
- Validating Your OTP Token
- Enrolling a New SafeNet eToken Virtual Temp

Updating Your Token Content

Update your token content for any of the following reasons:

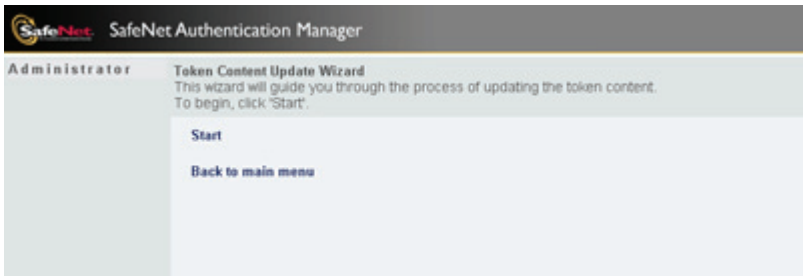
- You accidentally deleted content from your token.
- Your administrator asked you to update your token content.
- You want to change certain token details.
- A message was displayed that you should update your token content when one of the following occurred:
  - You accessed the Self Service Center
  - The SAM Agent determined that your token content must be updated
  - You verified your token content using the SAM Agent

Updating token content is identical to enrolling a new token, except that the token already exists in the SafeNet Authentication Manager inventory.

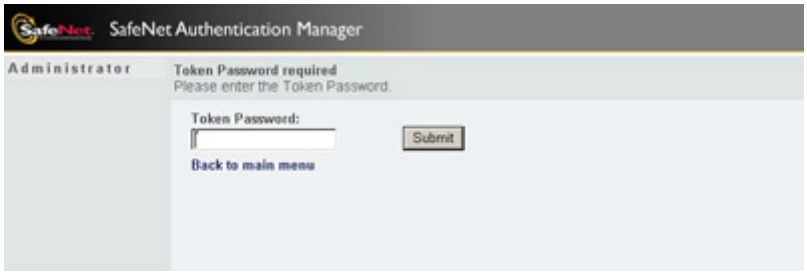
To update your token content:

1. Connect the token to be updated.
2. In the *Welcome to the Self Service Center* window, select the appropriate token, and select **Update the token content**.

   The *Token Content Update Wizard* opens.

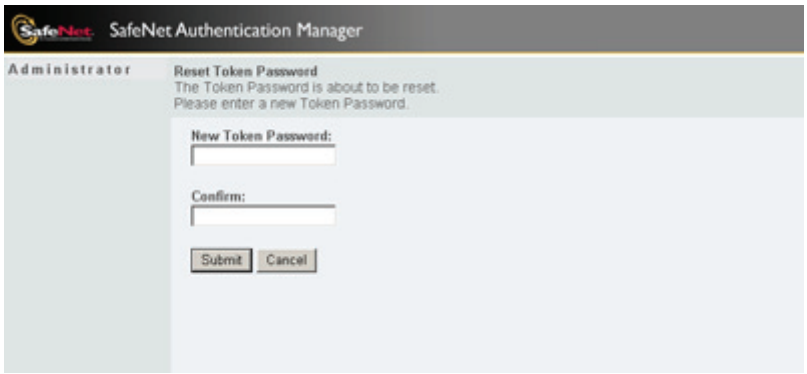


3. Click **Start**.
4. Depending on your SafeNet Authentication Manager configuration, you may be required to enter your Token Password.



Enter the Token Password, and click **Submit**.

5. Depending on your SafeNet Authentication Manager configuration, you may be required to set a new Token Password.



Enter a new Token Password, confirm it, and click **Submit**.

Tip:
It is your responsibility to remember your new Token Password. You must provide it to authenticate yourself when you access your token content.

Note:
Depending on your SafeNet Authentication Manager configuration, your Token Password may be required to comply with password quality settings, such as:

- minimum length
- inclusion or exclusion of lower-case letters, upper-case letters, numerals, and/or special characters
- disqualification of password values previously used

6. The *Set Token Name* window opens.

7. You may change the token name.
   In this example, the token name is changed to **Sarah's OTP Token**.

Tip:
If you have more than one token, we recommend assigning each one a unique token name.

8. Click **Submit**.
9. Depending on your SafeNet Authentication Manager configuration, you may need to do any of the following:
   - Enter a certificate password.
   - If you are enrolling an OTP token, set a new OTP PIN.
   - Enter and confirm your user password.

Click **Submit**.

Tip:
It is your responsibility to remember your new OTP PIN. You must provide it to authenticate yourself when you use your OTP.

10. When the enrollment is completed, the following information is displayed:
    - an *Enrollment successfully completed* message
    - the token name
    - other details

11. Click **Back to main menu** to return to the *Welcome to the Self Service Center* window.

Changing and Resetting Your Token Password

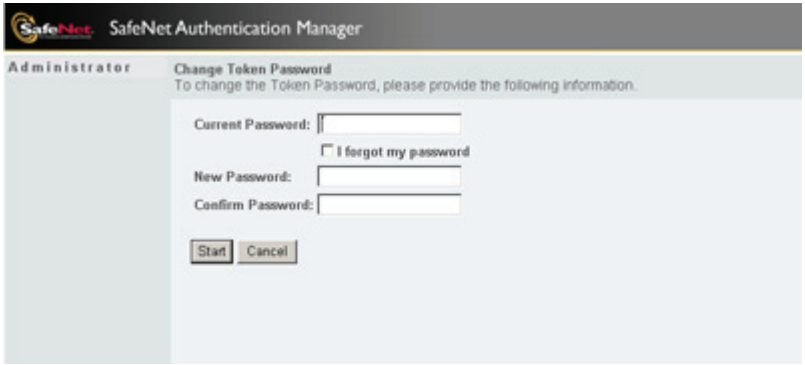
Change your password if it is about to expire, or if you think someone else has seen it.

Depending on your SafeNet Authentication Manager configuration, you may be able to reset your password if you forgot it.

To change or reset your Token Password:

1. In the *Welcome to the Self Service Center* window, select the appropriate token, and select **Change or reset the Token Password.**

   The *Change Token Password* window opens.



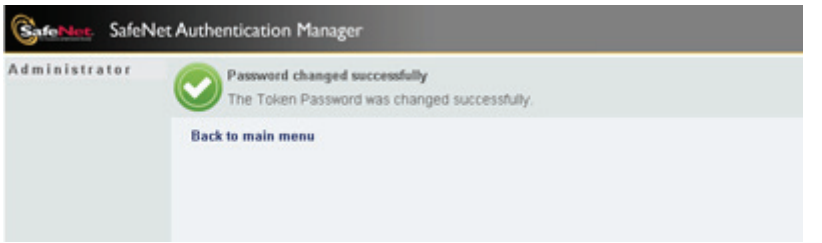
2. Do one of the following:
   - To change your Token Password, complete the *Current Password* field.
   - If your SafeNet Authentication Manager is configured to allow password reset, you can select **I forgot my password**.
3. Enter a new Token Password, confirm it, and click **Start**.

Tip:
It is your responsibility to remember your new Token Password. You must provide it to authenticate yourself when you access your token content.

Note:
Depending on your SafeNet Authentication Manager configuration, your Token Password may be required to comply with password quality settings, such as:

- minimum length
- inclusion or exclusion of lower-case letters, upper-case letters, numerals, and/or special characters
- disqualification of password values previously used

A *Password successfully changed* message is displayed.



4. Click **Back to main menu** to return to the *Welcome to the Self Service Center* window.

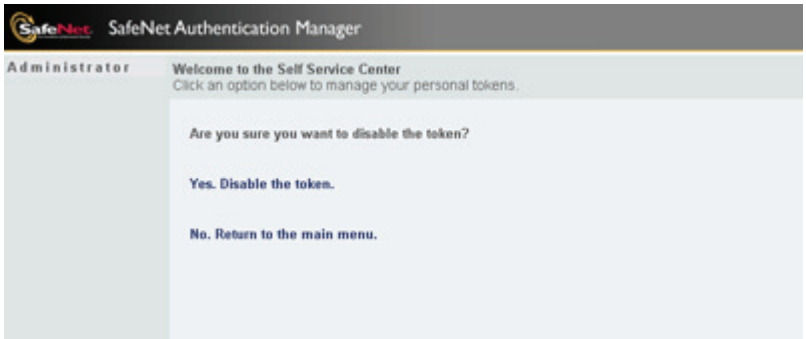
Enabling and Temporarily Disabling Your Token

For security reasons, you should temporarily disable your token if it is misplaced, or if it is not needed for an extended period.

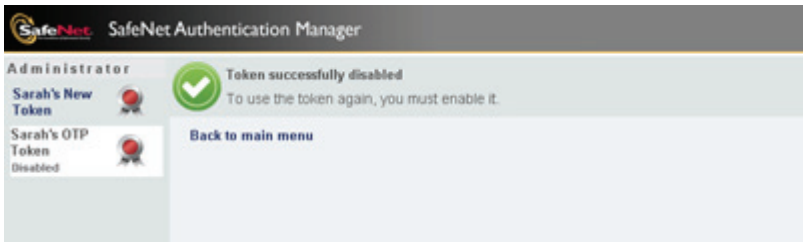
If your token is disabled, you must enable it before you can use it again.

To temporarily disable a token:

1. In the *Welcome to the Self Service Center* window, select the appropriate token, and select **Temporarily disable the token.**
   Options are displayed to confirm your request.



2. Select **Yes. Disable the token.**
   The token is marked as disabled, and a *Token successfully disabled* message is displayed.

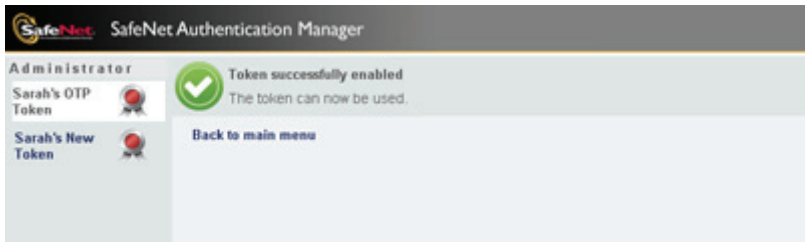


3. Click **Back to main menu** to return to the *Welcome to the Self Service Center* window.

To enable a token:

1. In the *Welcome to the Self Service Center* window, select the appropriate token, and select **Enable the disabled token.**

   The token is enabled, and a *Token successfully enabled* message is displayed.



2. Click **Back to main menu** to return to the *Welcome to the Self Service Center* window.

Revoking Your Lost or Damaged Token

For security reasons, you should report a lost or damaged token as soon as possible. A token that is reported as lost or damaged is marked as *Revoked* in the SafeNet Authentication Manager inventory. Its certificates, Network Logon profiles, and OTP can never be used again for authentication.

The information you provide when revoking your token is reported to your administrator.

If you already have a replacement token, and your token is not an OTP token, follow the instructions for replacing a lost or damaged token, instead of this section. For more information, see *Replacing or Upgrading Your Token* on page 75.

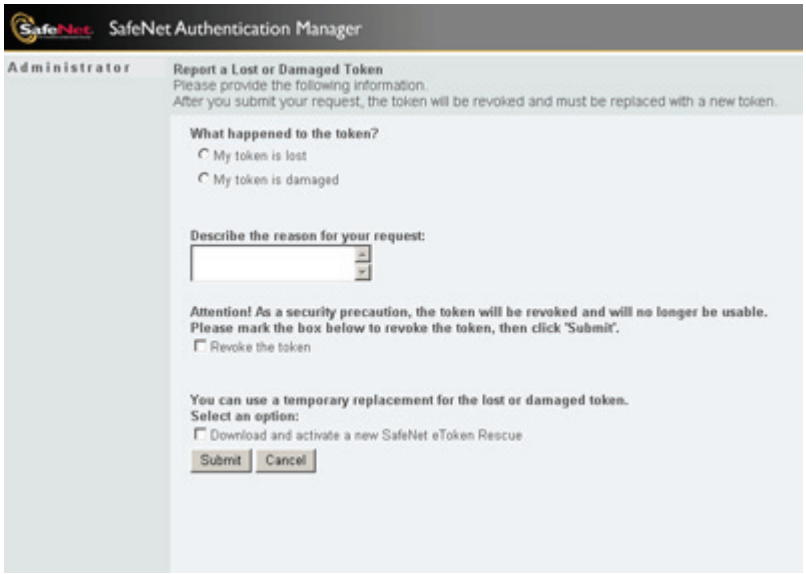
Note:
When a revoked token is replaced, new certificates, Network Logon profiles, and OTP generation replace those on the revoked token. Depending on your SafeNet Authentication Manager Configuration, some certificates from your revoked token are also loaded onto your new one.

Depending on your SafeNet Authentication Manager Configuration, you may download and activate a SafeNet eToken Rescue, a secure backup file on your computer or external device, to use in place of the reported token. For more information about SafeNet eToken Rescue tokens, see Chapter 1: *SafeNet eToken Rescue*, on page 6.

To revoke a lost or damaged token:

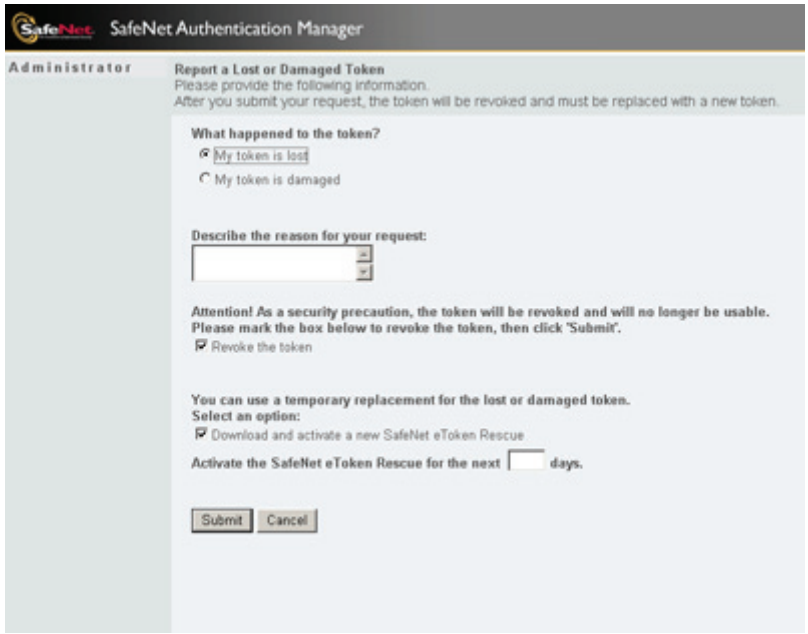
1. In the *Welcome to the Self Service Center* window, select the appropriate token, and select **Report the token as lost or damaged.**

   The *Report a Lost or Damaged Token* window opens.



2. Select one of the following:
   - **My token is lost**
   - **My token is damaged**
3. In the box, type a detailed reason for revoking your token.
4. Select **Revoke the token**.
5. Depending on your SafeNet Authentication Manager configuration, you may be able to select **Download and activate a new SafeNet eToken Rescue** to use in place of the reported token.

6. If you requested the activation of a SafeNet eToken Rescue, a prompt appears asking for the maximum number of days that you need to use it.

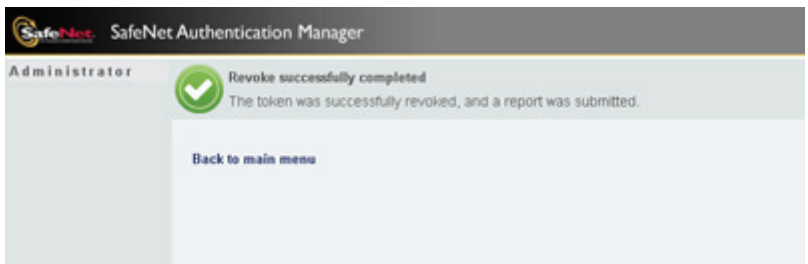


Enter the number of days that you need the SafeNet eToken Rescue to be functional.

Note:
A SafeNet eToken Rescue provides a lower level of security than a standard token. We recommend limiting its use to the number of days needed to acquire a new physical token.

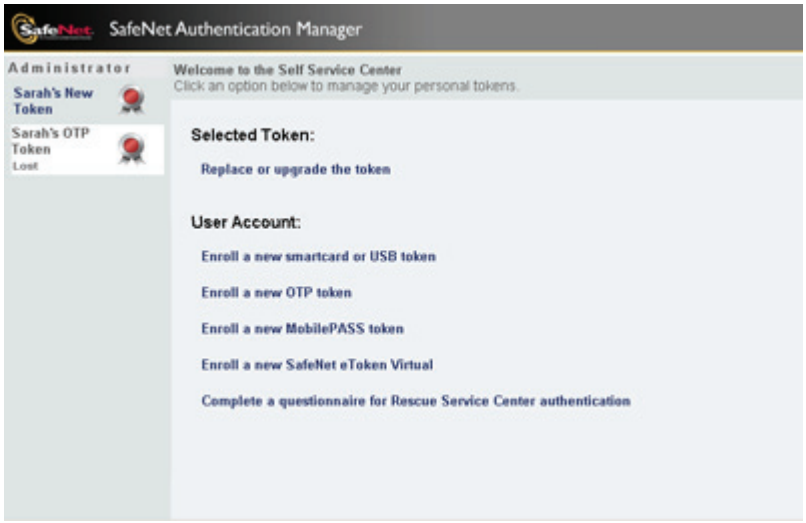
---

7. Click **Submit**.
8. If you did not request to download a SafeNet eToken Rescue, a *Revoke successfully completed* message is displayed.

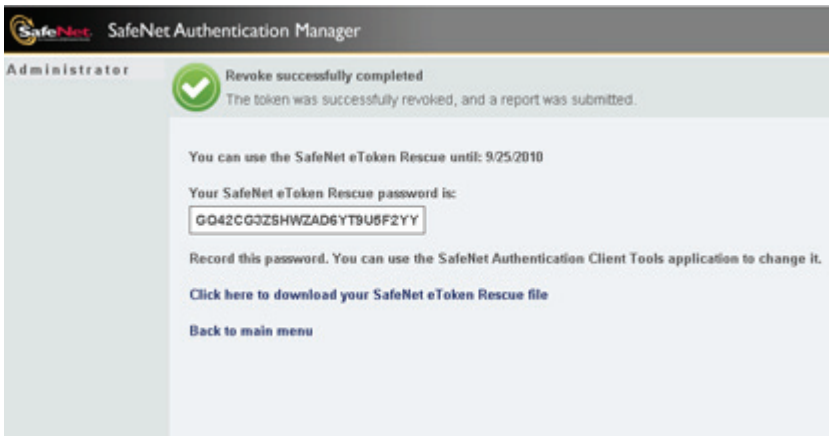


Click **Back to main menu** to return to the *Welcome to the Self Service Center* window.

In the left panel, the revoked token is marked as *Lost* or *Damaged*. Only one *Selected Token* option is displayed, allowing you to replace the token.



9. If you requested to download a SafeNet eToken Rescue, the following is displayed:
   - a *Revoke successfully completed* message
   - the SafeNet eToken Rescue expiration date
   - the SafeNet eToken Rescue password



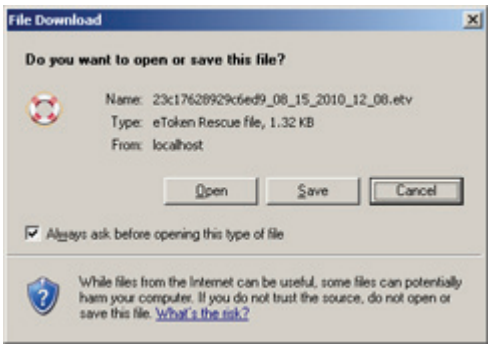
Do the following:

a. Write down the SafeNet eToken Rescue password, and save it in a safe place.

Tip:
It is your responsibility to remember your SafeNet eToken Rescue password. You may need to provide it to gain access to your SafeNet eToken Rescue content.
After your SafeNet eToken Rescue is opened, use the *SafeNet Authentication Client Tools* application to change the password to one that you can remember, yet no one else can know.

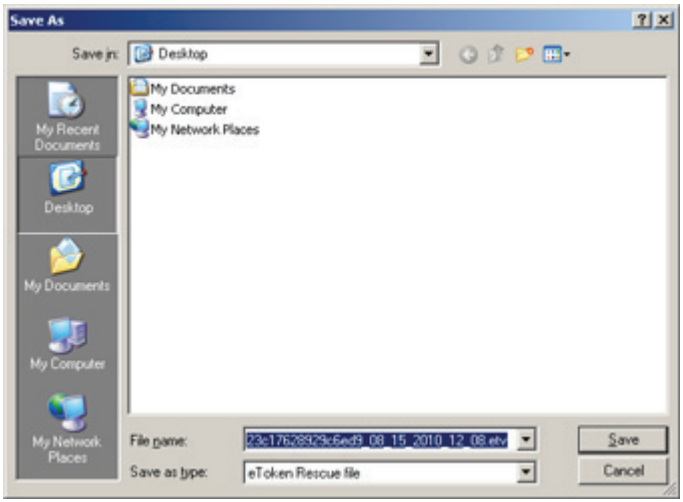
b. Click the link **Click here to download your SafeNet eToken Rescue file**.

The *File Download* window opens.



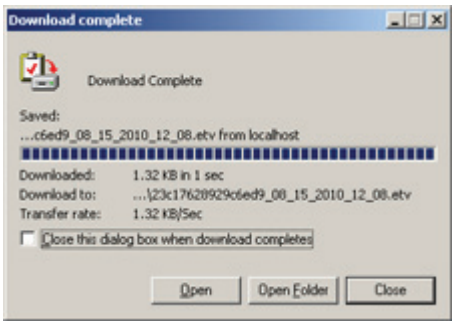
c. Click **Save**.

The *Save As* window opens.



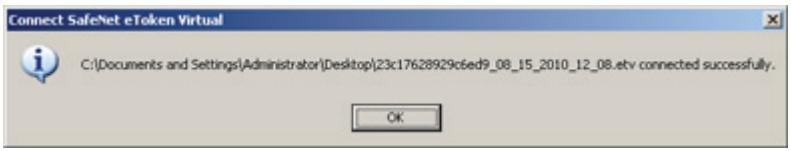
d. Select a location on your computer or external device to store the SafeNet eToken Rescue, and click **Save**.

The SafeNet eToken Rescue is saved, and the *Download Complete* window opens.



e. Click **Open** to define the file to SafeNet Authentication Client.

The SafeNet eToken Rescue is connected.



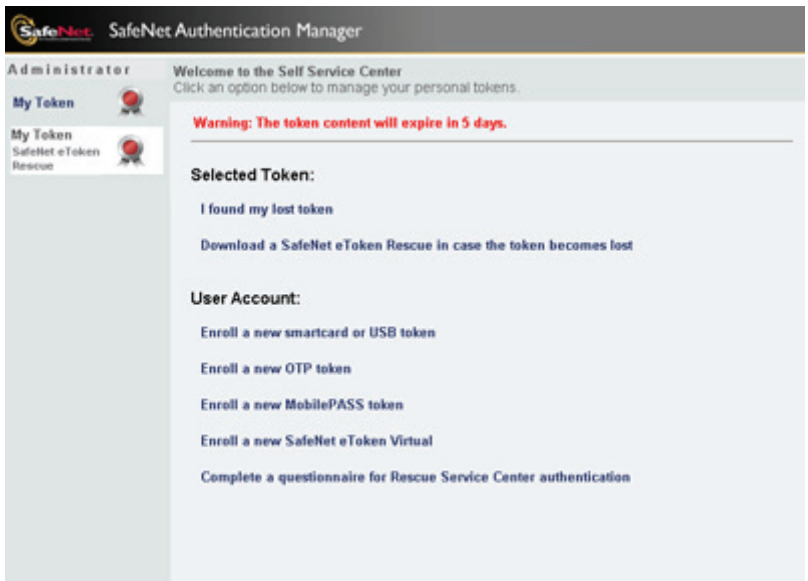
f. Click **OK** to close the dialog box.

The SafeNet eToken Rescue is saved to your computer or external device.

g. Click **Back to main menu** to return to the *Welcome to the Self Service Center* window.

The following is displayed:

- In the left panel, the revoked token is marked as *SafeNet eToken Rescue*.
- At the top of the right panel, a warning message displays when the token will expire.
- In the *Selected Token* area, options for the SafeNet eToken Rescue are displayed. For more information, see *Self Service Center Rescue Token Management* on page 93.



Replacing or Upgrading Your Token

This section describes how to:

- Replace a lost or damaged token with a new one
- Upgrade an outdated token by replacing it with a new model

When you replace or upgrade a token, the following steps take place:

a. If your old token is not revoked, SafeNet Authentication Manager revokes it.
b. The new token is added to the SafeNet Authentication Manager inventory if it is not already there.
c. The new token is associated with your username.
d. The new token is enrolled and loaded with the appropriate content to replace your revoked token. Depending on your SafeNet Authentication Manager configuration, this content may include:
   - Certificates
   - Network Logon profiles
   - OTP generation

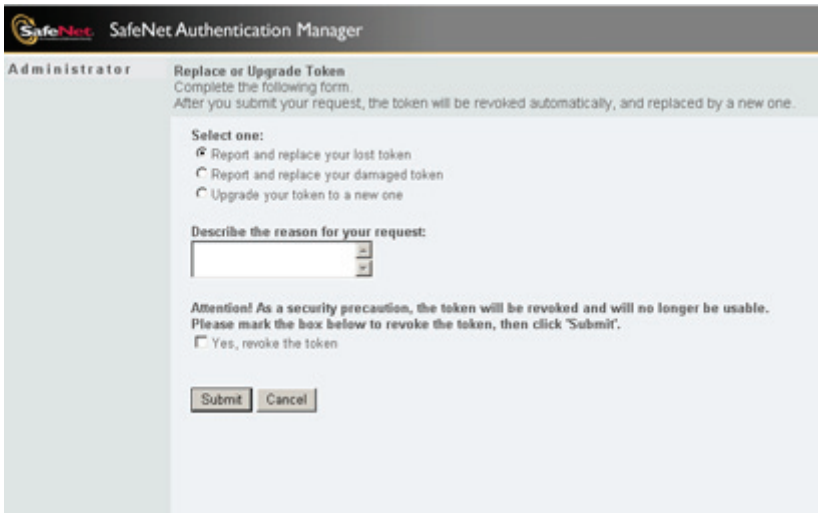
Note:
Restore other token content, such as WSO profiles, from backup files.

To replace or upgrade a non-USB OTP token:

1. Revoke your old OTP token. For more information, see *Revoking Your Lost or Damaged Token* on page 69.
2. Enroll your new OTP token. For more information, see *Enrolling a New OTP Token* on page 47.

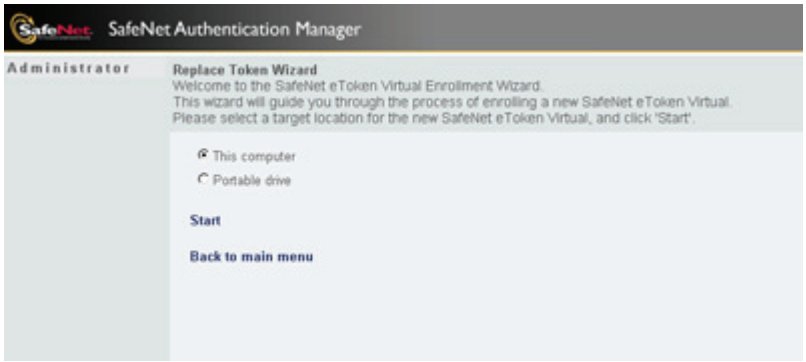
To replace or upgrade a token:

1. Connect the new token, and disconnect all others.
2. In the *Welcome to the Self Service Center* window, select the appropriate token, and select **Replace or upgrade the token**.
3. If the old token has not yet been revoked, the *Replace or Upgrade Token* window opens.



- If you are upgrading a token, select **Upgrade your token to a new one**, and click **Submit**.
- If you are replacing a token, do the following:
  a. Select one of the following:
     - **Report and replace your lost token**
     - **Report and replace your damaged token**
  b. In the box, type a detailed reason for revoking your token.
  c. Select **Yes, revoke the token**, and click **Submit**.

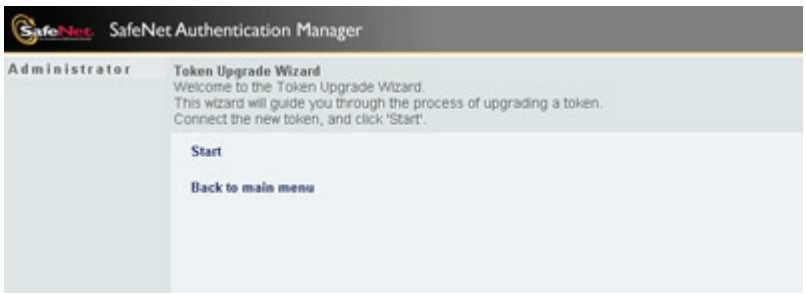
4. A wizard opens.
   - If you are replacing a token, the *Replace Token Wizard* opens.



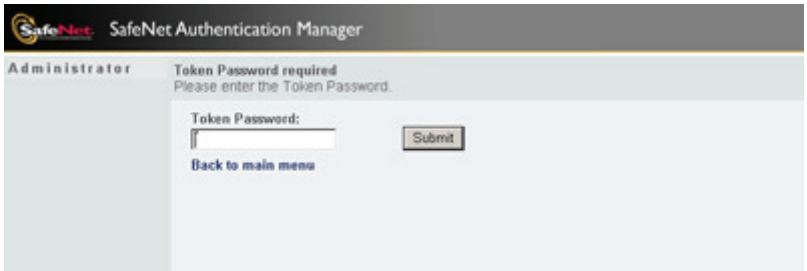
   If you are replacing a SafeNet eToken Virtual, you may be required to select the location of the new SafeNet eToken Virtual:
   - **This computer**
   - **Portable drive**

Note:
The portable drive must be connected.

   - If you are upgrading a token, the *Token Upgrade Wizard* opens.



5. Click **Start**.
6. Depending on your SafeNet Authentication Manager configuration, you may be required to enter the Token Password of the new token.

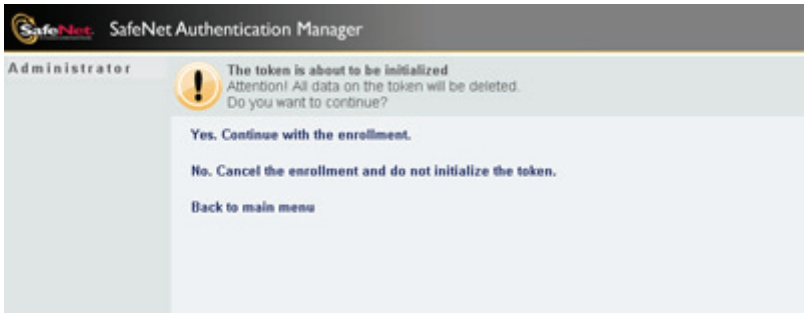


Enter the default Token Password used in your company, and click **Submit**.

Note:
The default Token Password is **1234567890**, unless your administrator has changed the default.

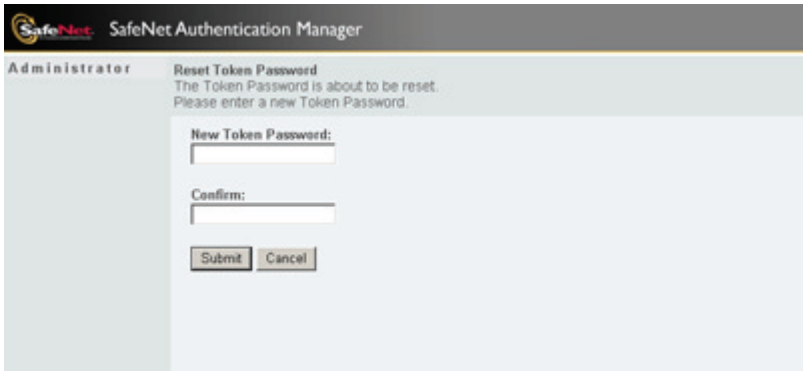
---

7. Depending on your SafeNet Authentication Manager configuration, a warning may be displayed that the token is about to be initialized.



Select **Yes. Continue with the enrollment**.

8. Depending on your SafeNet Authentication Manager configuration, you may be required to set a new Token Password.



Enter a Token Password that is different from the token's previous Token Passwords, confirm it, and click **Submit**.

Tip:
It is your responsibility to remember your new Token Password. You must provide it to authenticate yourself when you access your token content.

Note:
Depending on your SafeNet Authentication Manager configuration, your Token Password may be required to comply with password quality settings, such as:

- minimum length
- inclusion or exclusion of lower-case letters, upper-case letters, numerals, and/or special characters
- disqualification of password values previously used

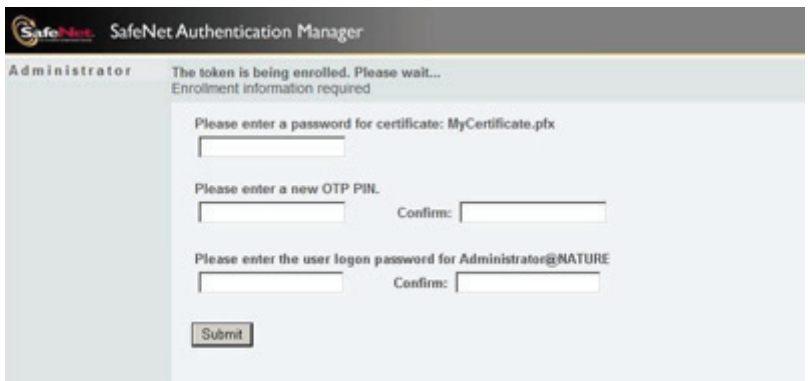
9. The *Set Token Name* window opens, displaying the default token name defined in your SafeNet Authentication Manager configuration.

10. You may change the token name.

    In this example, the token name is changed to **Sarah's OTP Token**.

Tip:
If you have more than one token, we recommend assigning each one a unique token name.

11. Click **Submit**.
12. Depending on your SafeNet Authentication Manager configuration, you may need to do any of the following:
    - Enter a certificate password.
    - If you are enrolling an OTP token, set a new OTP PIN.
    - Enter and confirm your user password.



Click **Submit**.

Tip:
It is your responsibility to remember your new OTP PIN. You must provide it to authenticate yourself when you use your OTP.

13. When the enrollment is completed, the following information is displayed:
    - an *Enrollment successfully completed* message
    - the token name
    - other details

Note:
If the details displayed are incorrect, you can change them by updating the token content. For more information, see *Updating Your Token Content* on page 62.

14. Click **Back to main menu** to return to the *Welcome to the Self Service Center* window.

Downloading a SafeNet eToken Rescue

You can save your token content to a *SafeNet eToken Rescue*, a secure backup file on your computer or external device. A SafeNet eToken Rescue is a SafeNet eToken Virtual product that can be activated for use as a temporary token replacement if your token is lost or damaged.

Download a SafeNet eToken Rescue file each time you leave on a trip so that the most up-to-date token content is backed up and available to you.

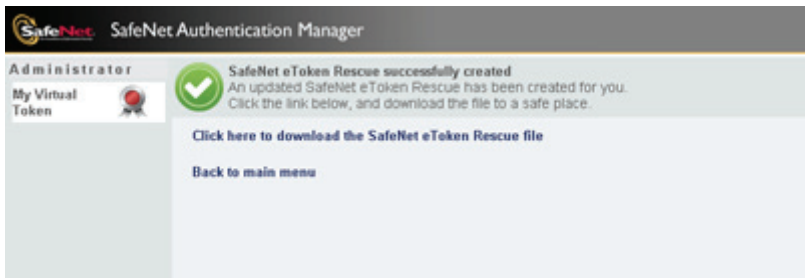
If your token is lost or damaged when you are away from your office, contact your administrator, or use the Rescue Service Center to report your lost token and to activate your SafeNet eToken Rescue. Then use your SafeNet eToken Rescue as you would use your physical token.

For more information about SafeNet eToken Rescue tokens, see Chapter 1: *SafeNet eToken Rescue*, on page 6.

To download a SafeNet eToken Rescue:

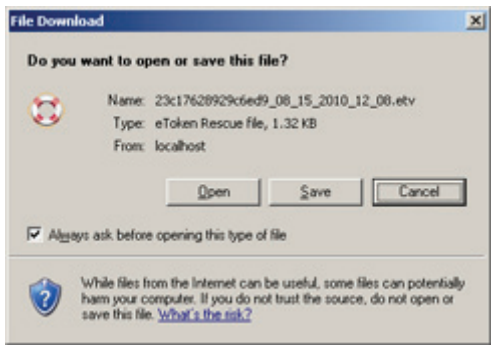
1. In the *Welcome to the Self Service Center* window, select the appropriate token, and select **Download a SafeNet eToken Rescue in case the token becomes lost**.

   A *SafeNet eToken Rescue successfully created* message is displayed.



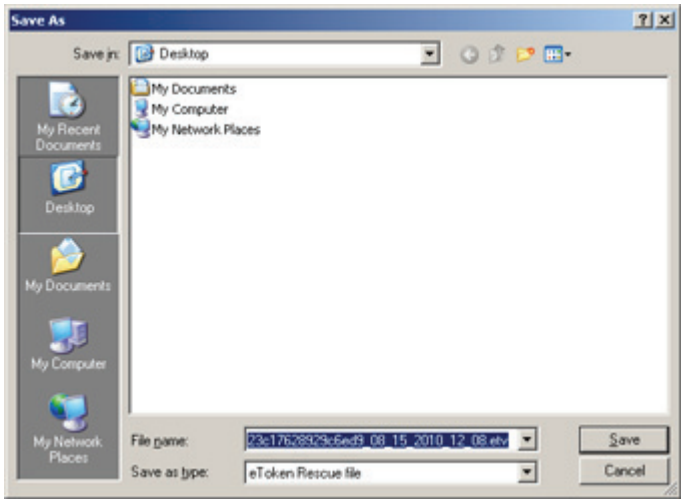
2. Click the link **Click here to download the SafeNet eToken Rescue file**.

   The *File Download* window opens.



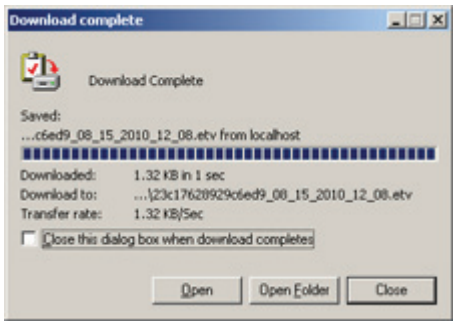
3. Click **Save**.

The *Save As* window opens.



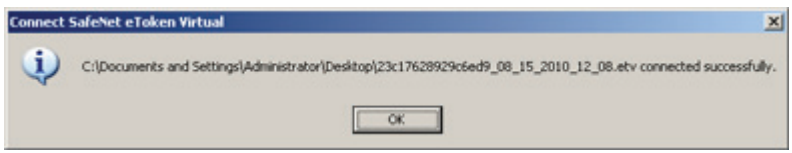
4. Select a location on your computer or external device to store the SafeNet eToken Rescue, and click **Save**.

   The SafeNet eToken Rescue is saved, and the *Download Complete* window opens.



5. Click **Open** to define the file to SafeNet Authentication Client.

   The SafeNet eToken Rescue is connected.



6. Click **OK** to close the dialog box.
7. Click **Back to main menu** to return to the *Welcome to the Self Service Center* window.

Changing and Resetting Your OTP PIN

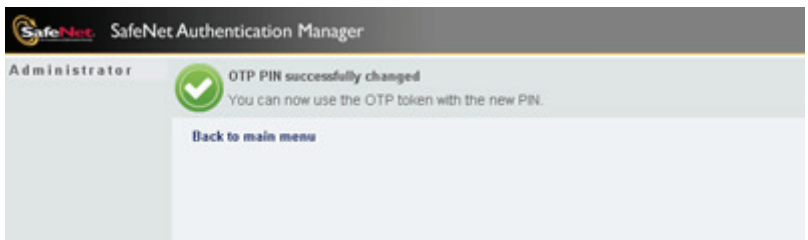
Change your OTP PIN if you think someone else has seen it.

Depending on your SafeNet Authentication Manager configuration, you may be able to reset your OTP PIN if you forgot it.

To change or reset your OTP PIN:

1. In the *Welcome to the Self Service Center* window, select the appropriate token, and select **Change or reset the OTP PIN.**
   The *Change OTP PIN* window opens.

2. Do one of the following:
   - To change your OTP PIN, complete the *Current PIN* field.
   - If your SafeNet Authentication Manager is configured to allow OTP PIN reset, you can select **I forgot my PIN**.
3. Enter a new OTP PIN, confirm it, and click **Start**.
   An *OTP PIN successfully changed* message is displayed.



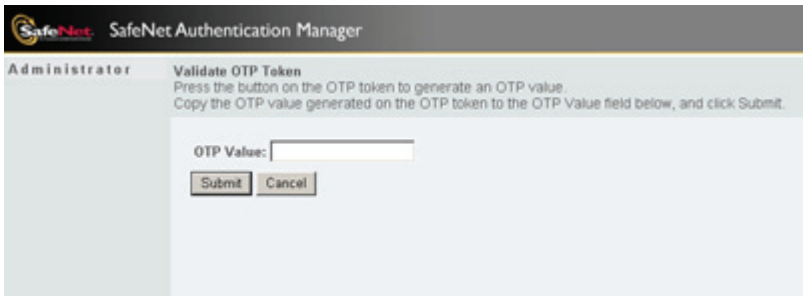
4. Click **Back to main menu** to return to the *Welcome to the Self Service Center* window.

Validating Your OTP Token

If you repeatedly generate an OTP without submitting one for authentication, or if the time function of your OTP token has deviated, your OTP token loses its synchronization with the system. You must validate your OTP token so that SafeNet Authentication Manager can authenticate a subsequently-generated OTP.

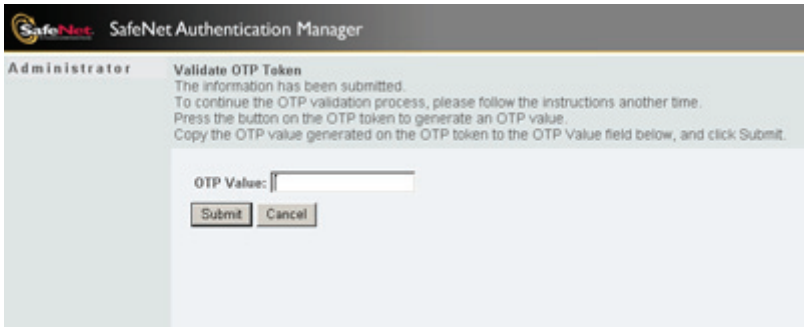
To validate your OTP token:

1. In the *Welcome to the Self Service Center* window, select the appropriate token, and select **Validate the OTP token.**
   The *Validate OTP Token* window opens.



2. Use your OTP token to generate an OTP value.
3. Depending on your SafeNet Authentication Manager configuration, enter one of the following into the **OTP Value** field:
   - OTP value generated on your token
   - OTP value generated on your token, preceded or followed by your OTP PIN
   - OTP value generated on your token, preceded or followed by your Windows password
4. Click **Submit**.
5. You may be requested to repeat step 2 through step 4 one or more times.

Tip:
You may need to wait until the previous OTP value fades from the token display before attempting to generate a new OTP value.



6. An *OTP validation successfully completed* message is displayed.
7. Click **Back to main menu** to return to the *Welcome to the Self Service Center* window.

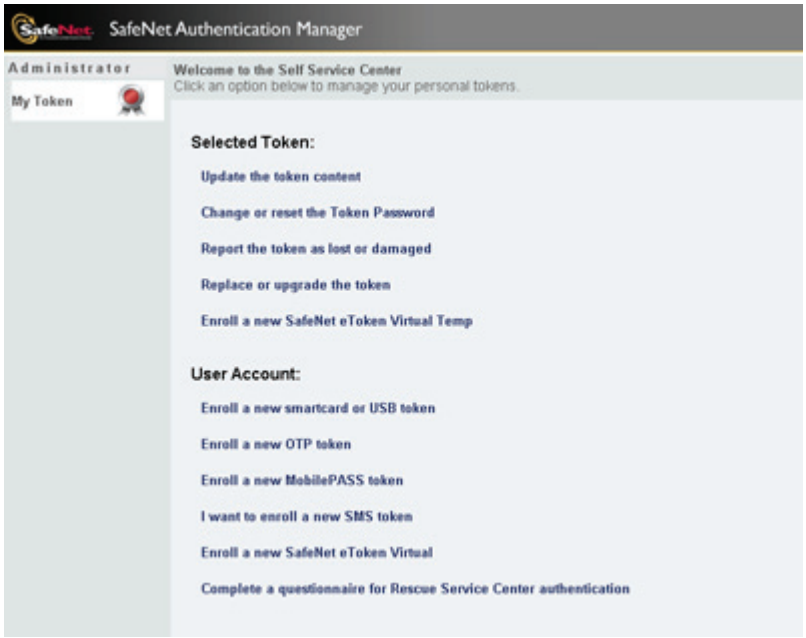
Enrolling a New SafeNet eToken Virtual Temp

SafeNet eToken Virtual Temp enrollment creates a software token on your computer that can be used temporarily in place of an enrolled token.

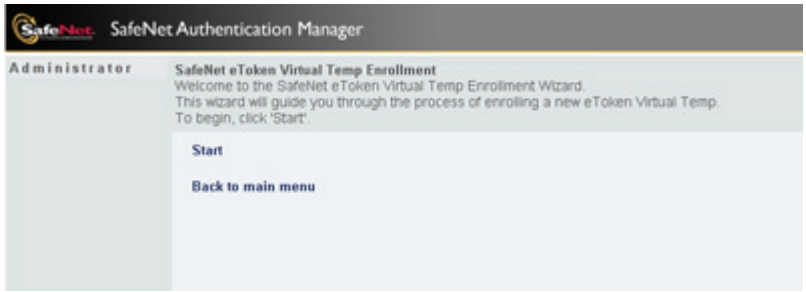
For more information, see Chapter 1, *SafeNet eToken Virtual Products*, on page 5.

To enroll a new SafeNet eToken Virtual Temp:

1. Disconnect all tokens.
2. In the *Welcome to the Self Service Center* window, select the token to be temporarily replaced by a SafeNet eToken Virtual Temp, and select **Enroll a new SafeNet eToken Virtual Temp**.

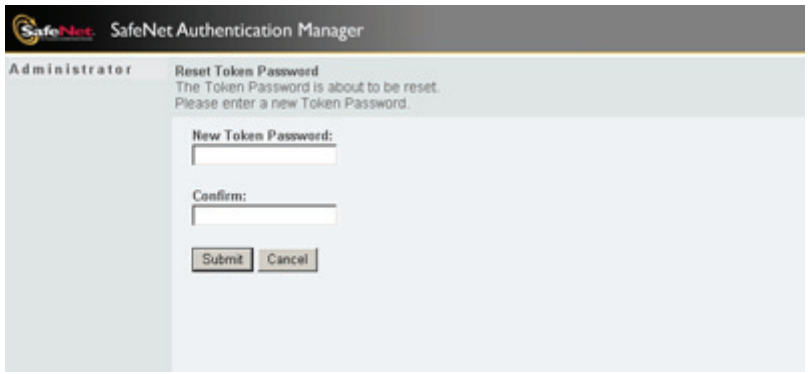


The *SafeNet eToken Virtual Temp Enrollment Wizard* opens.



3. Click **Start**.

4. Depending on your SafeNet Authentication Manager configuration, you may be required to set a new Token Password.



Enter a new Token Password, confirm it, and click **Submit**.

Tip:
It is your responsibility to remember your new Token Password. You must provide it to authenticate yourself when you access your token content.

Note:
Depending on your SafeNet Authentication Manager configuration, your Token Password may be required to comply with password quality settings, such as:

- minimum length
- inclusion or exclusion of lower-case letters, upper-case letters, numerals, and/or special characters
- disqualification of password values previously used

5. The *Set Token Name* window opens.

6. You may change the SafeNet eToken Virtual Temp name.
   In this example, the token name is changed to **My Temp Token**.

Tip:
If you have more than one token, we recommend assigning each one a unique token name.

7. Click **Submit**.
8. Depending on your SafeNet Authentication Manager configuration, you may need to do any of the following:
   - Enter a certificate password.
   - If you are enrolling an OTP token, set a new OTP PIN.
   - Enter and confirm your user password.

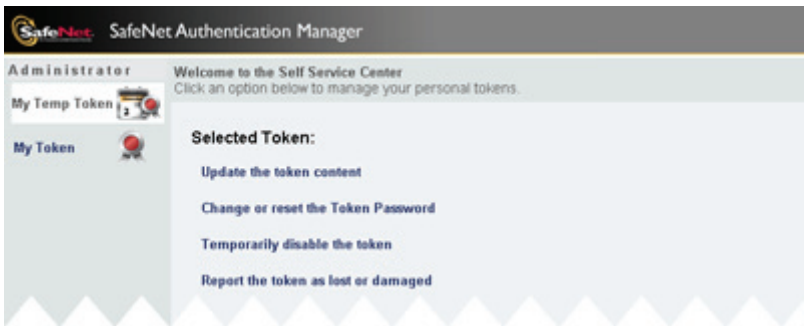
Click **Submit**.

Tip:
It is your responsibility to remember your new OTP PIN. You must provide it to authenticate yourself when you use your OTP.

9. When the enrollment is completed, the following information is displayed:
   - an *Enrollment successfully completed* message
   - the token name
   - other details

10. Click **Back to main menu** to return to the *Welcome to the Self Service Center* window.

    The name of the enrolled token is displayed in the left panel.



Chapter 6

Self Service Center Rescue Token Management

Use SafeNet Authentication Manager's Self Service Center to manage activities relating to your SafeNet eToken Rescue token.

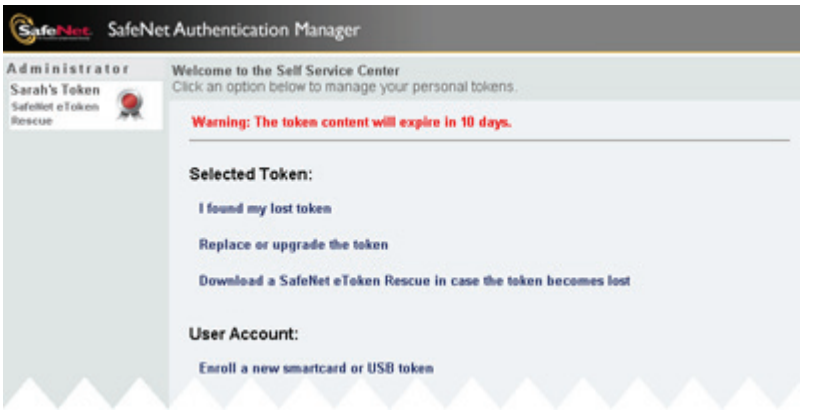
For more information about SafeNet eToken Rescue tokens, see Chapter 1, *SafeNet eToken Rescue*, on page 6.

In this chapter:

- Main Menu
- Re-enrolling a Lost Token
- Replacing a Lost Token
- Downloading a Backup SafeNet eToken Rescue

Main Menu

If the token selected in the *Welcome to the Self Service Center* window is a SafeNet eToken Rescue, relevant options are displayed.



Right Panel

The right panel includes messages relating to the selected SafeNet eToken Rescue.

The *Selected Token* options displayed in the right panel may include:

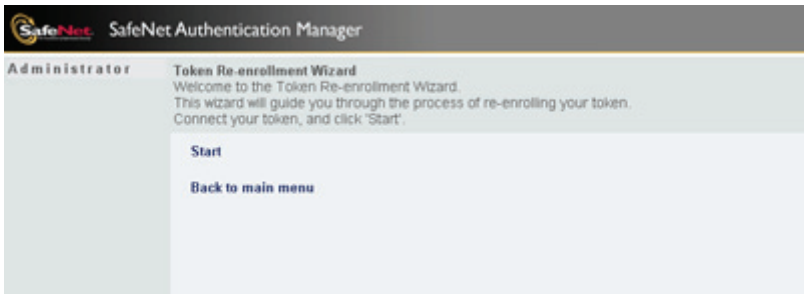
- Re-enrolling a Lost Token
  Enroll the original token that has been found.
- Replacing a Lost Token
  Enroll a new token in place of the original token.
- Downloading a Backup SafeNet eToken Rescue
  Download the backup file of your token content again.

Re-enrolling a Lost Token

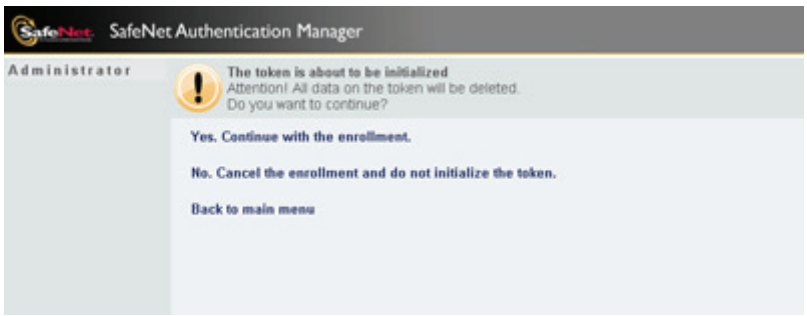
When the original token has been found, re-enroll it so that it can be used again. During the token re-enrollment, the SafeNet eToken Rescue is revoked and becomes unusable.

To re-enroll your found token:

1. Connect the found token.
2. In the *Welcome to the Self Service Center* window, select the appropriate token, and select **I found my lost token**.
   The *Token Re-enrollment Wizard* opens.

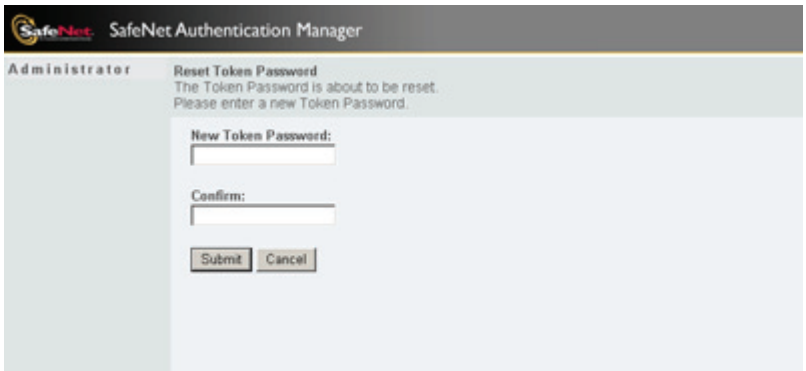


3. Click **Start**.
4. A warning is displayed that the token is about to be initialized.



   Select **Yes. Continue with the enrollment**.

5. Depending on your SafeNet Authentication Manager configuration, you may be required to set a new Token Password.



Enter a Token Password that is different from the token's previous Token Passwords, confirm it, and click **Submit**.

Tip:
It is your responsibility to remember your new Token Password. You must provide it to authenticate yourself when you access your token content.

Note:
Depending on your SafeNet Authentication Manager configuration, your Token Password may be required to comply with password quality settings, such as:

- minimum length
- inclusion or exclusion of lower-case letters, upper-case letters, numerals, and/or special characters
- disqualification of password values previously used

6. The *Set Token Name* window opens.

7. You may change the token name.
8. Click **Submit**.
9. Depending on your SafeNet Authentication Manager configuration, you may need to do any of the following:
   - Enter a certificate password.
   - If you are enrolling an OTP token, enter the token's current OTP PIN, and set a new OTP PIN.
   - Enter and confirm your user password.

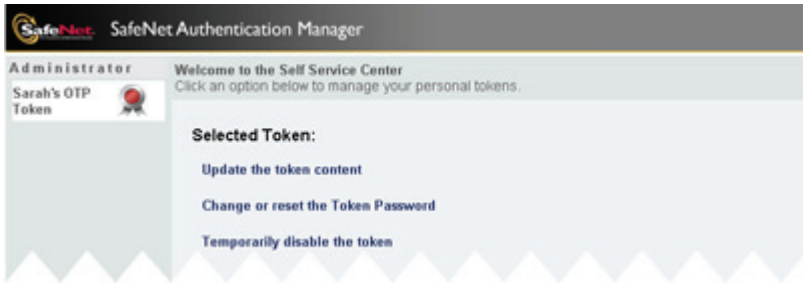
Click **Submit**.

Tip:
It is your responsibility to remember your new OTP PIN. You must provide it to authenticate yourself when you use your OTP.

10. When the enrollment is completed, the following information is displayed:
    - an *Enrollment successfully completed* message
    - the token name
    - other details

11. Click **Back to main menu** to return to the *Welcome to the Self Service Center* window.

    The found token has been re-enrolled and is displayed in the left panel.



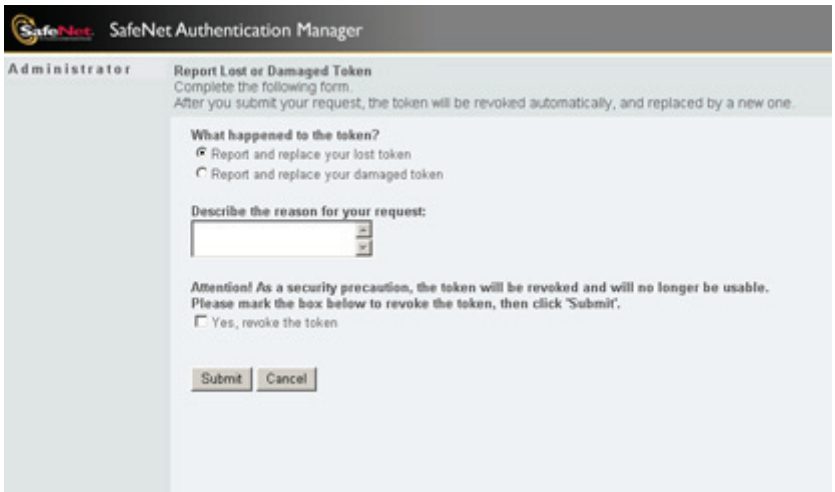
12. Select an option from the right panel, or close the browser to exit the Self Service Center.

Replacing a Lost Token

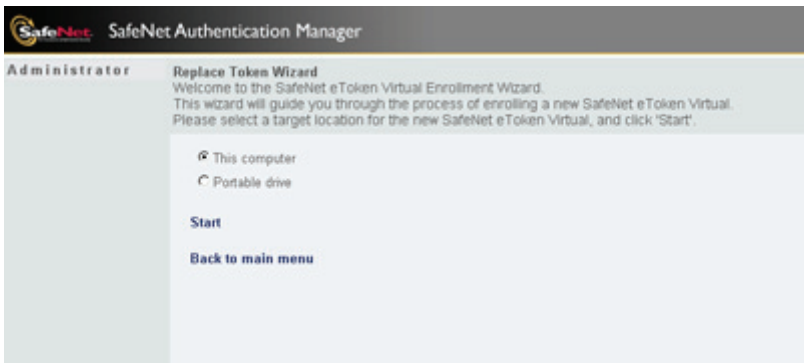
When the original token is damaged or cannot be found, replace it with a different token. During the enrollment of the replacement token, the SafeNet eToken Rescue is revoked and becomes unusable.

To replace a lost or damaged token:

1. Connect the new token, and disconnect all others.
2. In the *Welcome to the Self Service Center* window, select the appropriate token, and select **Replace or upgrade the token**.
3. The *Replace Lost or Damaged Token* window opens.



4. Select one of the following:
   - **Report and replace your lost token**
   - **Report and replace your damaged token**
5. In the box, type a detailed reason for revoking your token.
6. Select **Yes, revoke the token**, and click **Submit**.
7. The *Replace Token Wizard* opens.

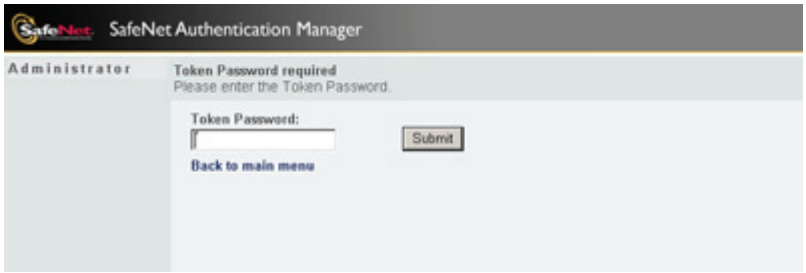


If you are replacing a SafeNet eToken Virtual, you may be required to select the location of the new SafeNet eToken Virtual:

- **This computer**
- **Portable drive**

Note:
The portable drive must be connected.

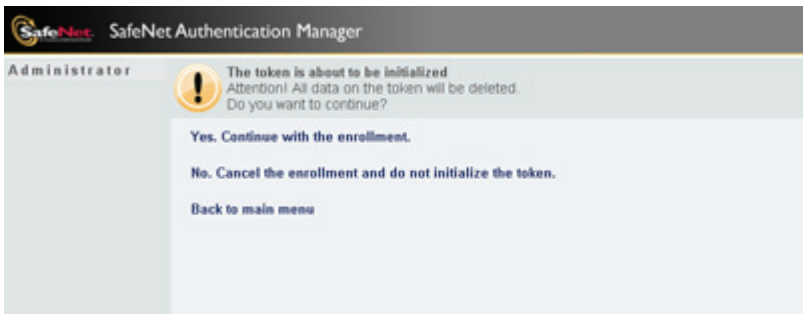
8. Click **Start**.
9. Depending on your SafeNet Authentication Manager configuration, you may be required to enter the Token Password.



Enter the default Token Password used in your company, and click **Submit**.

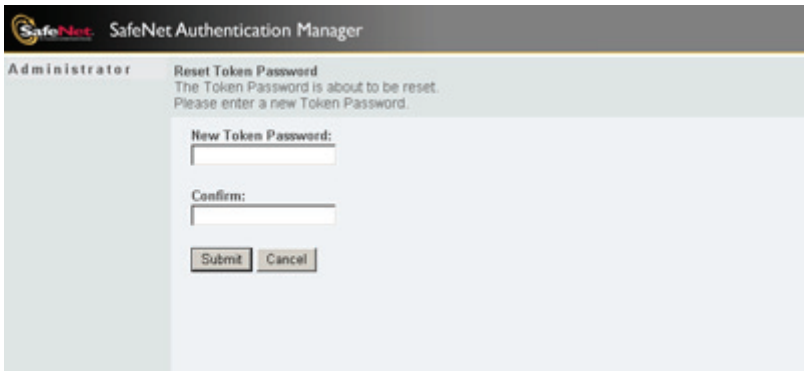
Note:
The default Token Password is **1234567890**, unless your administrator has changed the default.

10. Depending on your SafeNet Authentication Manager configuration, a warning may be displayed that the token is about to be initialized.



Select **Yes. Continue with enrollment**.

11. Depending on your SafeNet Authentication Manager configuration, you may be required to set a new Token Password.



Enter a Token Password that is different from the token's previous Token Passwords, confirm it, and click **Submit**.

Tip:
It is your responsibility to remember your new Token Password. You must provide it to authenticate yourself when you access your token content.

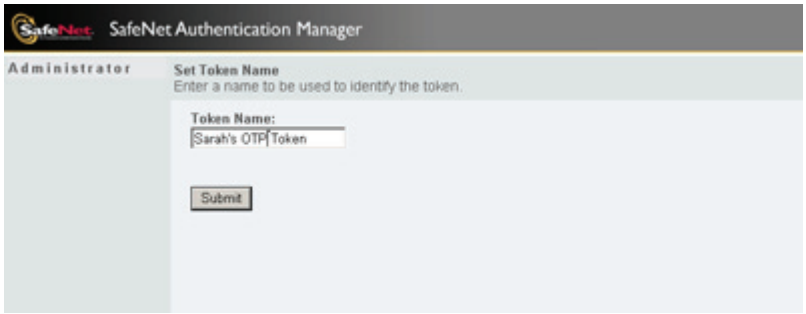
Note:
Depending on your SafeNet Authentication Manager configuration, your Token Password may be required to comply with password quality settings, such as:

- minimum length
- inclusion or exclusion of lower-case letters, upper-case letters, numerals, and/or special characters
- disqualification of password values previously used

12. The *Set Token Name* window opens, displaying the default token name defined in your SafeNet Authentication Manager configuration.

13. You may change the token name.

    In this example, the token name is changed to **Sarah's OTP Token**.



Tip:
If you have more than one token, we recommend assigning each one a unique token name.

14. Click **Submit**.
15. Depending on your SafeNet Authentication Manager configuration, you may need to do any of the following:
    - Enter a certificate password.
    - If you are enrolling an OTP token, set a new OTP PIN.
    - Enter and confirm your user password.

Click **Submit**.

Tip:
It is your responsibility to remember your new OTP PIN. You must provide it to authenticate yourself when you use your OTP.

16. When the enrollment is completed, the following information is displayed:
    - an *Enrollment successfully completed* message
    - the token name
    - other details

Note:
If the details displayed are incorrect, you can change them by updating the token content. For more information, see *Main Menu* on page 94.

17. Click **Back to main menu** to return to the *Welcome to the Self Service Center* window.

Downloading a Backup SafeNet eToken Rescue

You can save your SafeNet eToken Rescue's token content to a different *SafeNet eToken Rescue* on your computer or external device. For more information, see *Downloading a SafeNet eToken Rescue* on page 82.

Part III Rescue Service Center

The following chapters describe how to use SafeNet Authentication Manager's Rescue Service Center.

In this section:

- Chapter 7: Rescue Service Center (page 107)
- Chapter 8: Rescue Service Center Token Activities (page 113)
- Chapter 9: Rescue Service Center Rescue Token Management (page 131)

Chapter 7

Rescue Service Center

SafeNet Authentication Manager's Rescue Service Center is a web-based application for users who are away from their office and are unable to use their token due to specific problems.

In this chapter:

- Rescue Service Center Overview
- Accessing the Rescue Service Center Main Menu

Rescue Service Center Overview

The Rescue Service Center provides a solution for situations in which you are out of the office and cannot contact your administrator. Use the Rescue Service Center to perform certain actions which can normally be performed only by an administrator.

The Rescue Service Center covers situations in which you need help with your token or SafeNet eToken Rescue, such as:

- You forgot your Token Password
- Your token is damaged or lost
- You need to temporarily disable your token
- You need to enable your temporarily disabled token
- You need access to your downloaded SafeNet eToken Rescue
- You no longer need your SafeNet eToken Rescue

If your token is an OTP token, you can do the following:

- Reset your OTP PIN
- Validate your OTP token

Accessing the Rescue Service Center Main Menu

You must complete an authentication questionnaire in the Self Service Center before you can use the Rescue Service Center. For more information, see Chapter 4, *Completing Your Authentication Questionnaire*, on page 57.

Access the Rescue Service Center through your company's server.

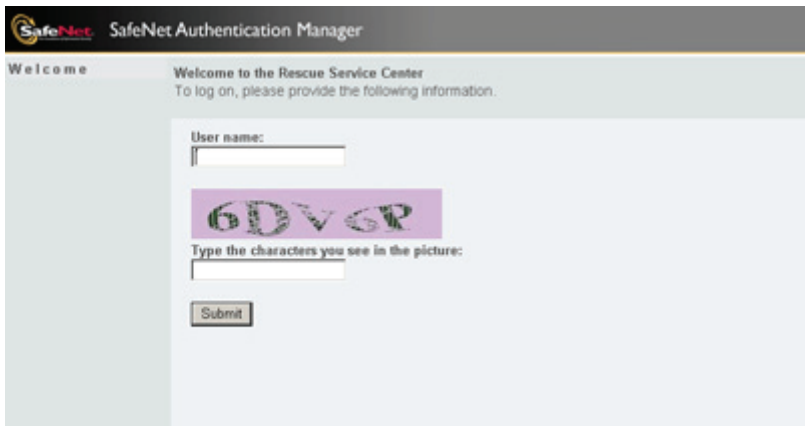
Note:
Each company has its own SafeNet Authentication Manager server. This guide uses **localhost** to represent your company's SafeNet Authentication Manager server. When following the steps in the procedure, replace **<localhost>** with the name of your company's SafeNet Authentication Manager server.

To access the Rescue Service Center main menu:

1. Open your web browser, and go to http://<localhost>/SAMRescue where **<localhost>** is the name of your company's SafeNet Authentication Manager server.

   Note:
   For the website to display properly, ensure that the browser's *Text Size* is set to *Medium*.
   a. On the browser toolbar, click **View**.
   b. From the dropdown menu, select **Text Size** > **Medium**.

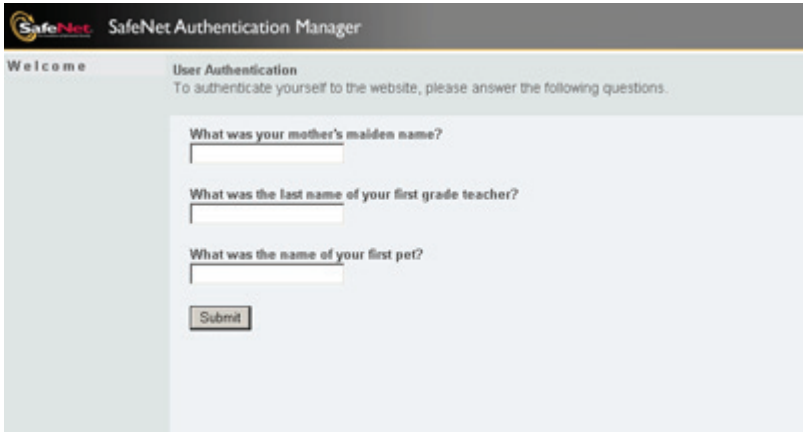
   The *Welcome to the Rescue Service Center* authentication window opens.



2. Enter your username, type the text shown in the picture, and click **Submit**.

   Note:
   The text is not case-sensitive.

The *User Authentication* window opens, displaying questions you answered in the Self Service Center.

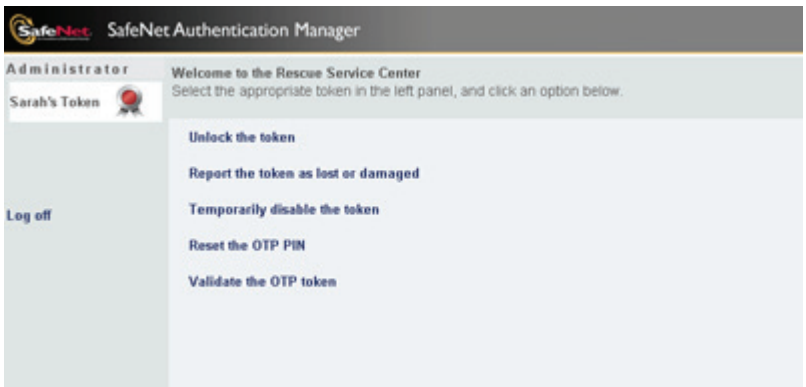


Note:
Each company defines its own authentication questions. The questionnaire shown is an example.

3. Enter the same responses you provided to the Self Service Center, and click **Submit**.

Note:
The answers are not case-sensitive.

When the answers are authenticated, The *Welcome to the Rescue Service Center* options window opens.



- If you have no enrolled tokens, the following message is displayed at the top of the Rescue Service Center window:

  No tokens found

  You do not have any enabled tokens.
- If you have at least one enrolled token, a list of your tokens is displayed in the left panel of the Rescue Service Center window, below your user name. The list includes the names of each of your tokens, their representative token images, and their status if not *Normal*. The selected token is highlighted.

4. Select the appropriate token in the left panel, and select an option from the right panel.

Note:
Your SafeNet Authentication Manager configuration determines which options are displayed in the right panel.

---

5. To exit the Rescue Service Center, click **Log Off** in the left panel.

Chapter 8

Rescue Service Center Token Activities

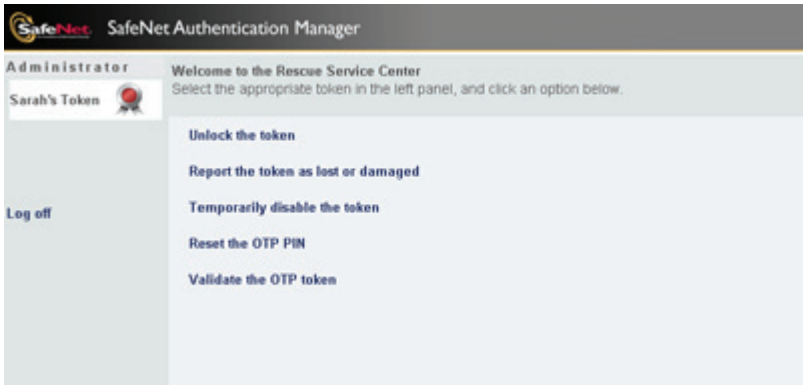
Use SafeNet Authentication Manager's Rescue Service Center to manage token activities when you are away from your office and are unable to use your token due to specific problems.

In this chapter:

- Main Menu
- Retrieving a Response Code to Unlock Your Token
- Managing Your Lost or Damaged Token
- Enabling and Temporarily Disabling Your Token
- Resetting Your OTP PIN
- Validating Your OTP Token

Main Menu

Unless the token selected in the *Welcome to the Rescue Service Center* window is a SafeNet eToken Rescue, some or all of the following options are displayed.



Right Panel

The options displayed in the right panel may include:

- Retrieving a Response Code to Unlock Your Token

  Complete the process of unlocking a token whose Token Password has been forgotten.

- Managing Your Lost or Damaged Token

  Report a lost or damaged token so that it cannot be used by anyone else, and optionally arrange for a temporary replacement.

- Enabling and Temporarily Disabling Your Token

  Temporarily disable your token if it is misplaced, or if it is not needed for an extended period.

  If your token is disabled, you must enable it before you can use it again.

- Resetting Your OTP PIN

  Reset your OTP PIN should you forget it.

- Validating Your OTP Token

  If you repeatedly generate an OTP without submitting one for authentication, or if the time function of your OTP token has deviated, your OTP token loses its synchronization with the system. You must validate your OTP token so that SafeNet Authentication Manager can authenticate OTPs that are generated.

Note:
Your SafeNet Authentication Manager configuration determines which options are displayed in the right panel.

Retrieving a Response Code to Unlock Your Token

If you forgot your Token Password, or if you consecutively entered an incorrect Token Password too many times, your token becomes locked.

Use the *Challenge - Response* system to do the following:

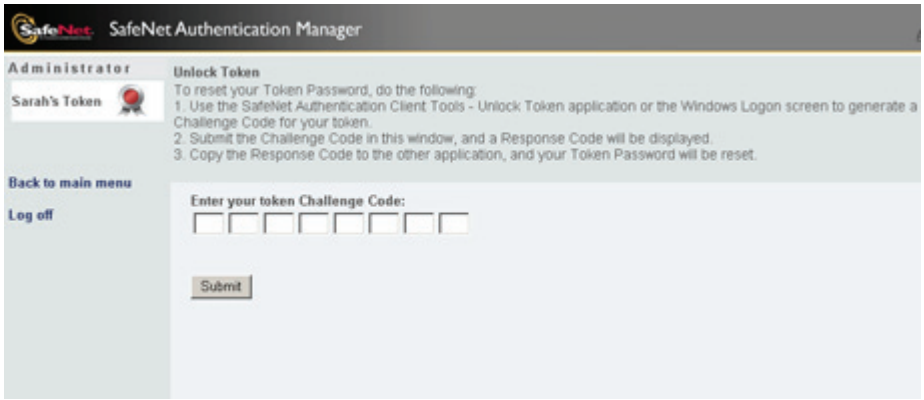
- Unlock your token
- Set a new Token Password

To unlock your token and set a new Token Password:

1. Select **Unlock token** in one of the following SafeNet applications:
   - *SafeNet Authentication Client Tools*
   - *eToken Network Logon*
2. Assign a new Token Password, and follow the *Unlock token* instructions until a **Challenge Code** is generated.

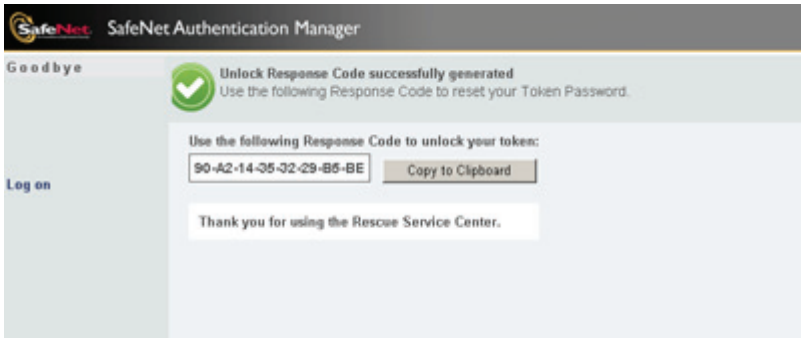
   Tip:
   It is your responsibility to remember your new Token Password.
3. Log on to the Rescue Service Center.
4. In the *Welcome to the Rescue Service Center* window, select **Unlock the token**.

The *Unlock Token* window opens.



5. Type the 16-character **Challenge Code** displayed on the *Unlock Token* window of your application, and click **Submit**.

   The *Unlock Response Code* window opens.



6. Record the displayed **Response Code**, or click **Copy to clipboard**.
7. Enter or paste the 16-character **Response Code** to the *Unlock Token* window of your application, and continue with that application.

Managing Your Lost or Damaged Token

For security reasons, you should report a lost or damaged token as soon as possible.

If your token becomes lost or damaged when you are away from your office, your SafeNet Authentication Manager configuration determines which of the following actions you can do through the Rescue Service Center:

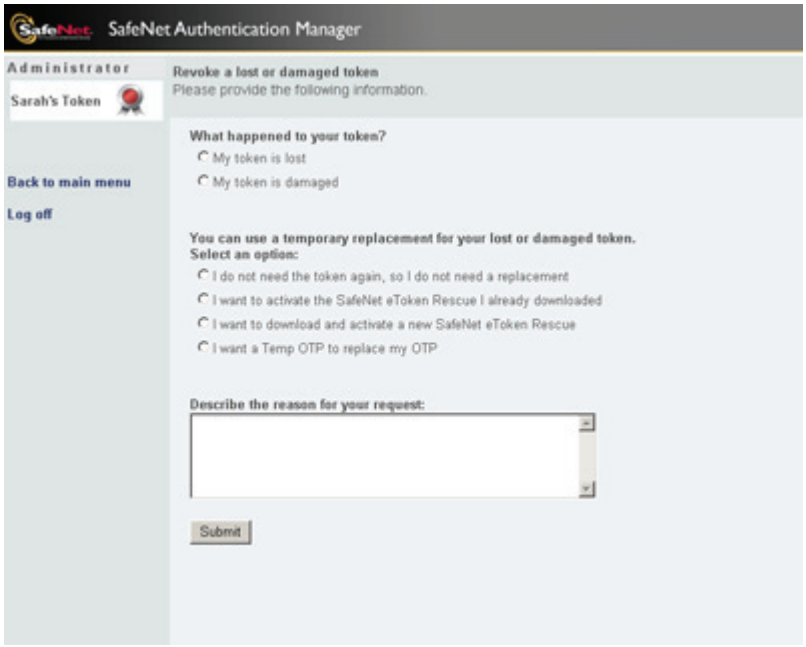
- If you do not need your token's content, set its status as one of the following:
  - **Revoked**: Select this option if your token is permanently unavailable to you. Your token can never be used again by anyone.
  - **Disabled**: Select this option if your token is temporarily unavailable to you. You can use your token again after you enable it.
- If you need to replace only the token's OTP function, request a *Temp OTP*. A Temp OTP is a static value to use in place of a generated OTP. Its value does not change, and so it provides a low level of security. It is valid for a limited time only.
- If you need to replace your token content, and you have not downloaded a *SafeNet eToken Rescue*, download one and activate it.
- If you need to replace your token content, and you already downloaded a *SafeNet eToken Rescue*, activate it.

Note:
A SafeNet eToken Rescue is a secure backup file on your computer or external device. It is used as a temporary token replacement. It is accessible for a limited time only, and only through a password that is disclosed when you report your token as lost or damaged.
For more information about SafeNet eToken Rescue tokens, see Chapter 1, *SafeNet eToken Rescue*, on page 6.

Reporting and Temporarily Replacing Your Lost or Damaged Token

To report your lost or damaged token, and optionally, to temporarily replace it:

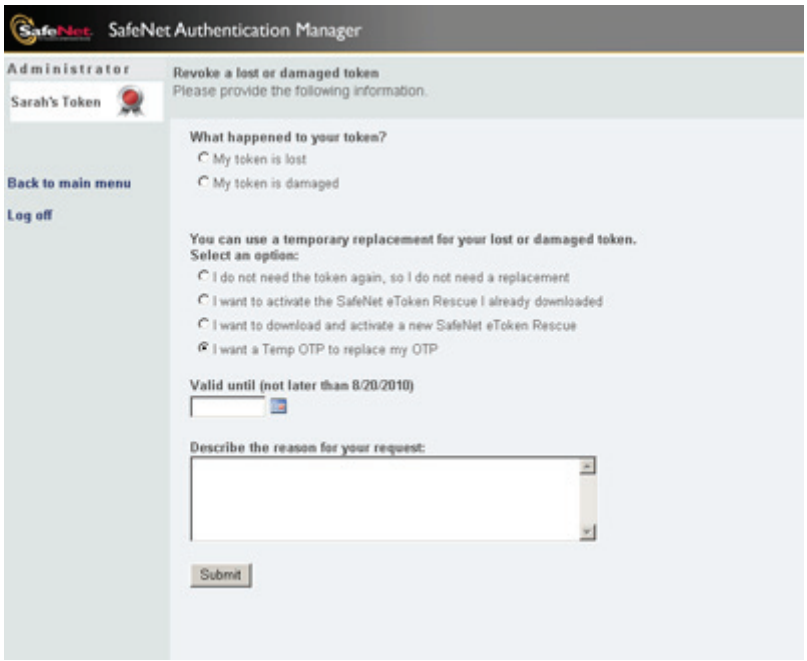
1. In the *Welcome to the Rescue Service Center* window, select **Report the token as lost or damaged**.
   The *Revoke a lost or damaged token* window opens.



2. Select the appropriate answer to *What happened to your token?*.
   - **My token is lost**
   - **My token is damaged**
3. Depending on your SafeNet Authentication Manager configuration, select one of the options displayed.
   - **I do not need that token again, so I do not need a replacement**
   - **I want to activate the SafeNet eToken Rescue I already downloaded**

- **I want to download and activate a new SafeNet eToken Rescue**
- **I want a Temp OTP to replace my OTP**

4. In the box, type details regarding your request.
5. If you requested an Temp OTP, a prompt appears asking for the Temp OTP expiration date.

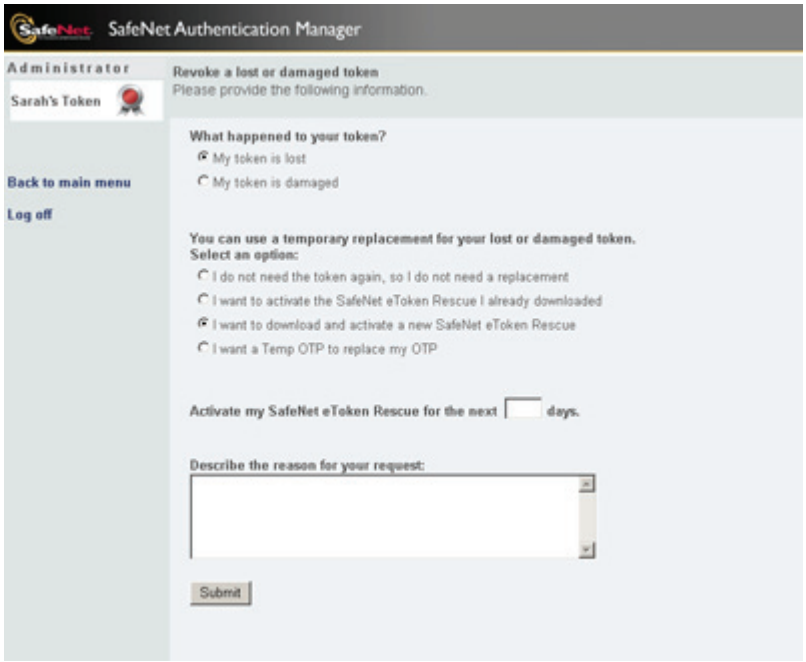


Enter or select the latest date that you will need the Temp OTP to be functional.

Note:
A Temp OTP provides a lower level of security than a standard OTP. We recommend limiting its use to the minimum number of days needed to acquire a new physical token.

---

6. If you requested the activation of a SafeNet eToken Rescue, a prompt appears asking for the maximum number of days that you need to use it.

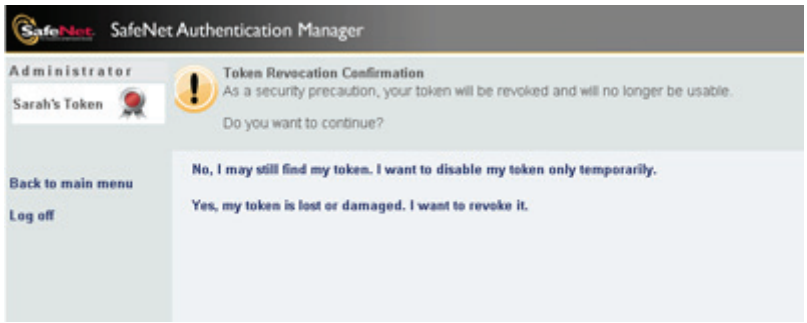


Enter the number of days that you need the SafeNet eToken Rescue to be functional.

Note:
A SafeNet eToken Rescue provides a lower level of security than a standard token. We recommend limiting its use to the number of days needed to acquire a new physical token.

7. Click **Submit**.

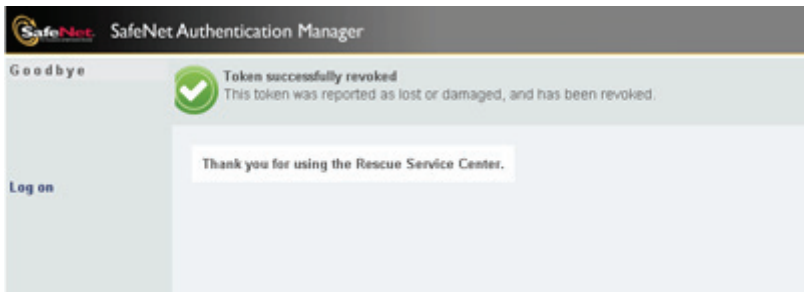
8. If you did not request access to a Temp OTP or a SafeNet eToken Rescue, a *Token Revocation Confirmation* window opens.



Do one of the following:

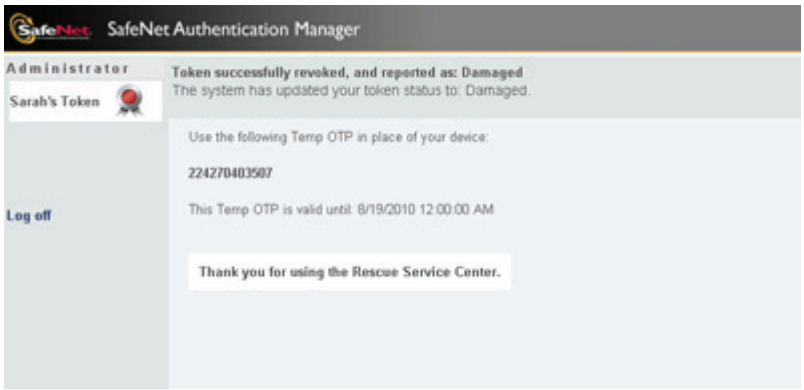
- To temporarily disable, but not permanently revoke, your lost token, select
  No, I may still find my token. I want to disable my token only temporarily.
- To permanently revoke your lost token so that it can never be used again, select
  Yes, my token is lost or damaged. I want to revoke it.
- To cancel the request to report your token as lost or damaged, click **Back to main menu.**

9. If you selected to revoke your token, the token status is displayed in the *Token successfully revoked* window.



10. If you requested a Temp OTP, the following Temp OTP information is displayed:
    - the Temp OTP value to use instead of a generated OTP
    - the Temp OTP expiration date

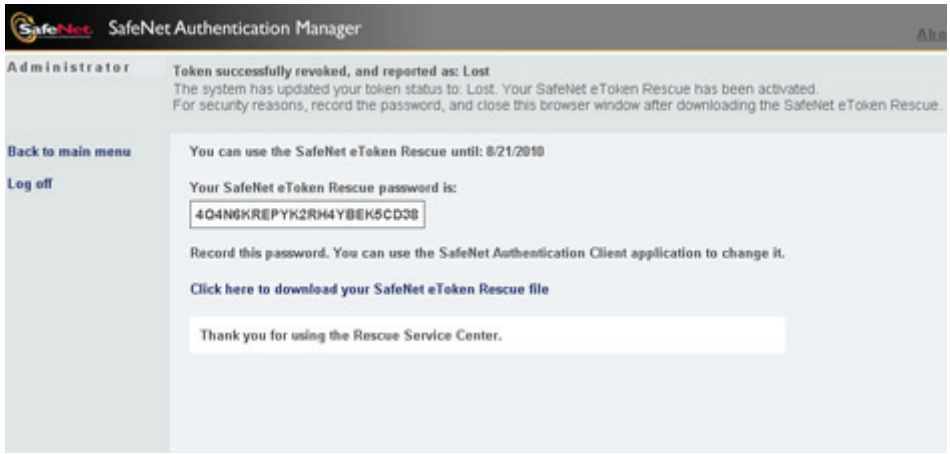
Note:
The expiration period of your Temp OTP is determined by your SafeNet Authentication Manager configuration.



Write down the Temp OTP value, and save it in a safe place.

Tip:
It is your responsibility to remember your new Temp OTP. During authentication, you must provide it in place of a generated OTP.

11. If you requested to download or activate a SafeNet eToken Rescue, the following information is displayed:
    - the SafeNet eToken Rescue expiration date
    - the SafeNet eToken Rescue password

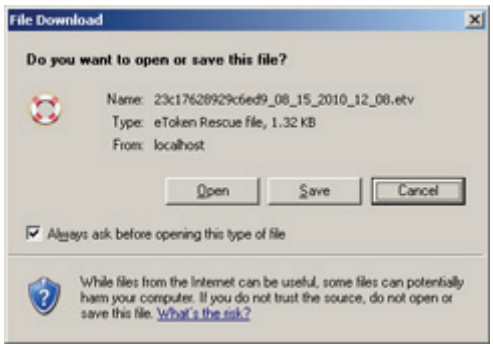


Write down the SafeNet eToken Rescue password, and save it in a safe place.

Tip:
It is your responsibility to remember your SafeNet eToken Rescue password. You may need to provide it to gain access to your SafeNet eToken Rescue content.
After your SafeNet eToken Rescue is opened, use the *SafeNet Authentication Client Tools* application to change the password to one that you can remember, yet no one else can know.

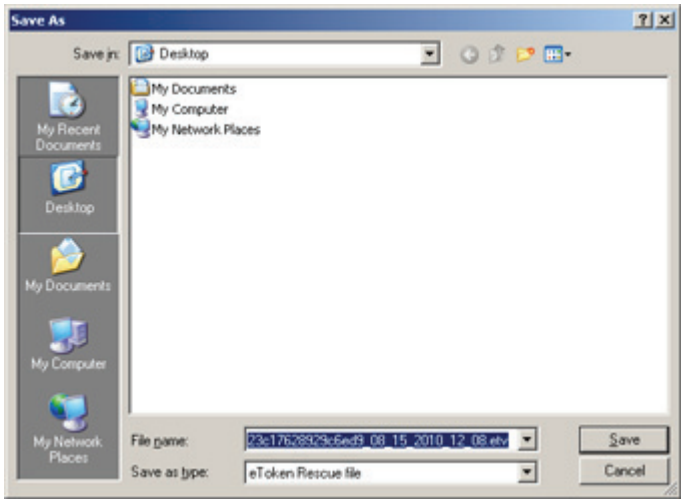
---

12. If you requested to download a SafeNet eToken Rescue, click the link **Click here to download your SafeNet eToken Rescue file**.
    The *File Download* window opens.



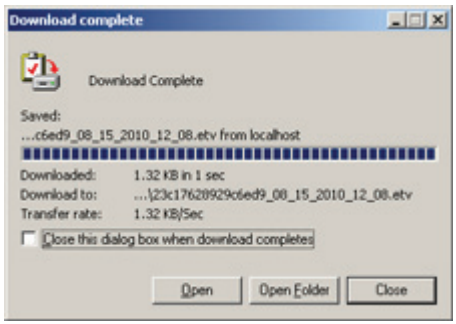
13. Click **Save**.

The *Save As* window opens.



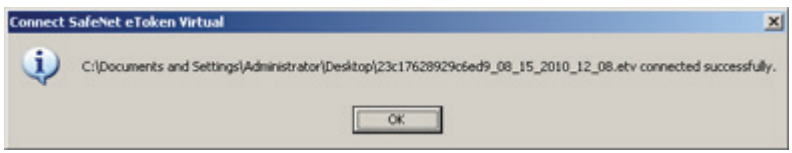
14. Select a location on your computer or external device to store the SafeNet eToken Rescue, and click **Save**.

    The SafeNet eToken Rescue is saved, and the *Download Complete* window opens.



15. Click **Open** to define the file to SafeNet Authentication Client.

    The SafeNet eToken Rescue is connected.



16. Click **OK** to close the dialog box.

The SafeNet eToken Rescue is saved to your computer or external device.

Replacing Your Token with a New Token

When you return to your office, do the following:

1. Ask your administrator to give you a new token in place of your lost one.
2. Log on to the *Self Service Center* through your company's server.
3. If you had access to a Temp OTP or a SafeNet eToken Rescue, revoke your token by selecting **Report the token as lost or damaged**.
4. Do one of the following actions to replace your revoked token with the new one:
   - If your token is a non-USB OTP device, select **Enroll a new OTP token.**
   - If your token is not an OTP device, select **Replace or upgrade the token**.

Generating an OTP Using Your SafeNet eToken Rescue

To generate an OTP using a SafeNet eToken Rescue:

1. If the SafeNet eToken Rescue is not connected, browse to its location, right-click the filename, and click **Open** to define the file to *SafeNet Authentication Client*.
2. Right-click the *SafeNet Authentication Client* tray icon, and from the menu, select the SafeNet eToken Rescue token.
3. Right-click the *SafeNet Authentication Client* tray icon, and from the menu, select **Generate OTP**.

   The *Generate OTP* window opens.
4. Click **Generate OTP**.

   A message appears requesting the Token Password.
5. Enter the SafeNet eToken Rescue password.

   An OTP is generated and displayed.
6. Copy the OTP to your application to authenticate yourself.

Enabling and Temporarily Disabling Your Token

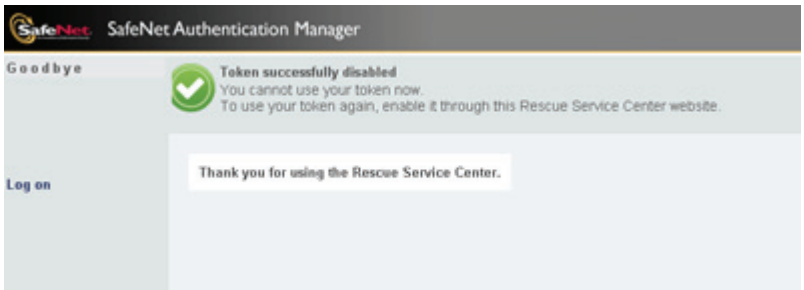
For security reasons, you should temporarily disable your token if it is misplaced, or if it is not needed for an extended period.

If your token is disabled, you must enable it before you can use it again.

To temporarily disable your token:

- In the *Welcome to the Rescue Service Center* window, select **Temporarily disable the token**.

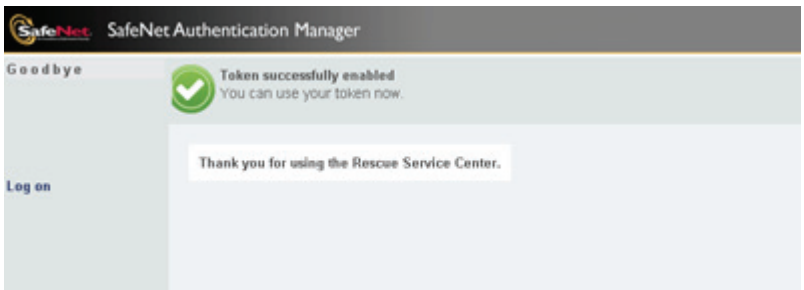
  The token is marked as disabled, and a *Token successfully disabled* message is displayed.



To enable your token:

- In the *Welcome to the Rescue Service Center* window, select **Enable the token**.

  The token is enabled, and a *Token successfully enabled* message is displayed.

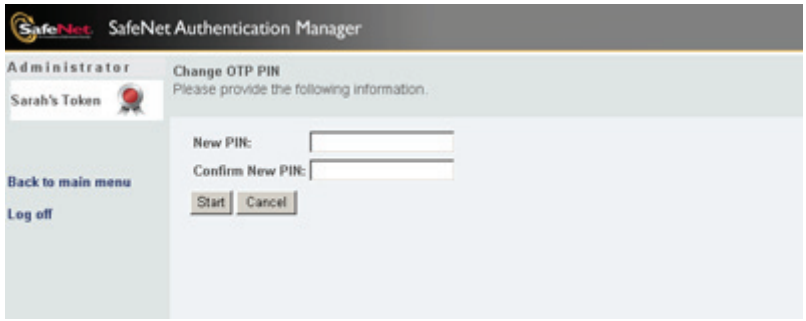


Resetting Your OTP PIN

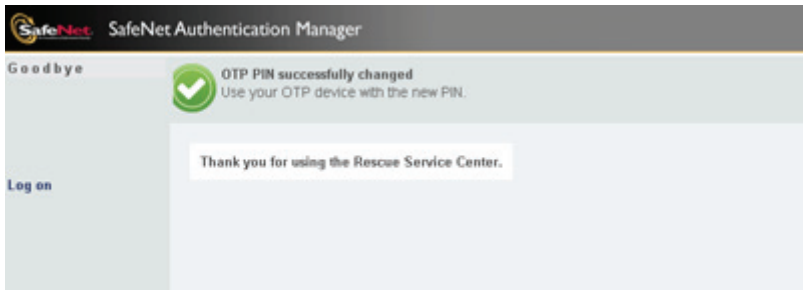
Reset your OTP PIN if you forgot it.

To reset your OTP PIN:

1. In the *Welcome to the Rescue Service Center* window, select **Reset the OTP PIN**.
   The *Change OTP PIN* window opens.



2. Enter a new OTP PIN, confirm it, and click **Start**.
   An *OTP PIN successfully changed* message is displayed.

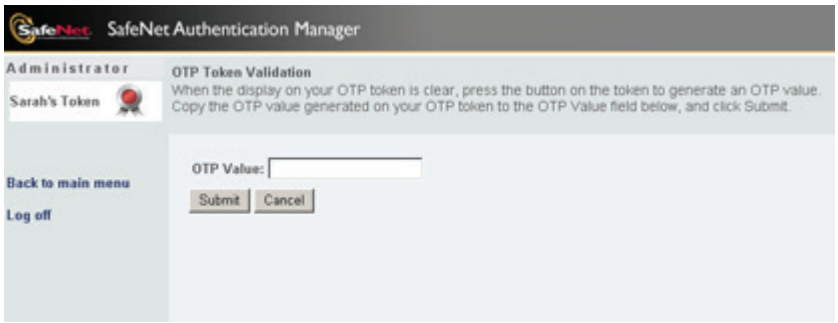


Validating Your OTP Token

If you repeatedly generate an OTP without submitting one for authentication, or if the time function of your OTP token has deviated, your OTP token loses its synchronization with the system. You must validate your OTP token so that SafeNet Authentication Manager can authenticate a subsequently-generated OTP.

To validate your OTP token:

1. In the *Welcome to the Rescue Service Center* window, select **Validate the OTP token.**
   The *OTP Token Validation* window opens.



2. Use your OTP token to generate an OTP value, enter it in the **OTP Value** field, and click **Submit**.
3. You may be requested to repeat step 2 one or more times.

Tip:
You may need to wait until the previous OTP value fades from the token display before attempting to generate a new OTP value.

4. Click **Submit**.
   An *OTP validation successfully completed* message is displayed.

Chapter 9

Rescue Service Center Rescue Token Management

Use SafeNet Authentication Manager's Rescue Service Center to manage activities relating to your SafeNet eToken Rescue token when you are away from the office.

For more information about SafeNet eToken Rescue tokens, see Chapter 1, *SafeNet eToken Rescue*, on page 6.

In this chapter:

- Main Menu
- Recovering Your SafeNet eToken Rescue Password
- Replacing Your SafeNet eToken Rescue
- Closing Your SafeNet eToken Rescue

Main Menu

If the token selected in the *Welcome to the Rescue Service Center* window is a SafeNet eToken Rescue, some or all of the following options are displayed.

Right Panel

The options displayed in the right panel may include:

- Recovering Your SafeNet eToken Rescue Password

  Recover the SafeNet eToken Rescue password that was provided during activation.

- Replacing Your SafeNet eToken Rescue

  Download another SafeNet eToken Rescue file to replace one already downloaded.

- Closing Your SafeNet eToken Rescue

  Close your activated SafeNet eToken Rescue when you no longer need it.

Recovering Your SafeNet eToken Rescue Password

If you cannot access your activated SafeNet eToken Rescue because you forgot its password, use the Rescue Service Center to recover the SafeNet eToken Rescue password that was provided during activation.

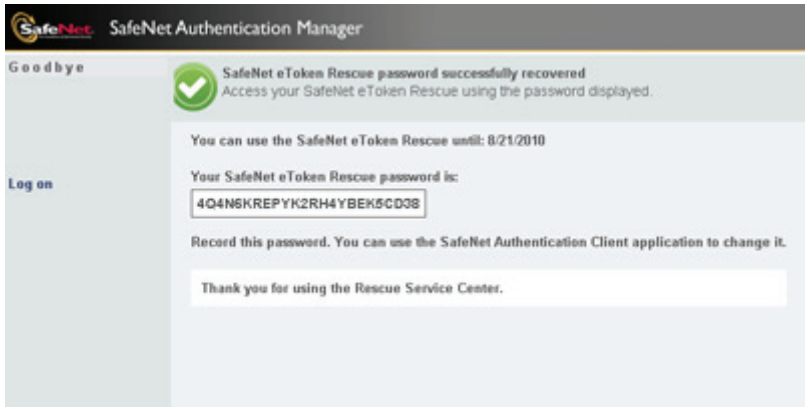
Note:
Only the original password can be recovered. If you changed the password, the new password cannot be recovered. You must download a new SafeNet eToken Rescue.

To recover your SafeNet eToken Rescue password:

1. In the *Welcome to the Rescue Service Center* window, select **Send me a new password for the SafeNet eToken Rescue**.

   The following information is displayed:

   - a *SafeNet eToken Rescue password successfully recovered* message
   - the SafeNet eToken Rescue expiration date
   - the SafeNet eToken Rescue password



2. Write down the SafeNet eToken Rescue password, and save it in a safe place.

Replacing Your SafeNet eToken Rescue

If you cannot locate the SafeNet eToken Rescue file that you already downloaded, or if you cannot recover its password, download another file.

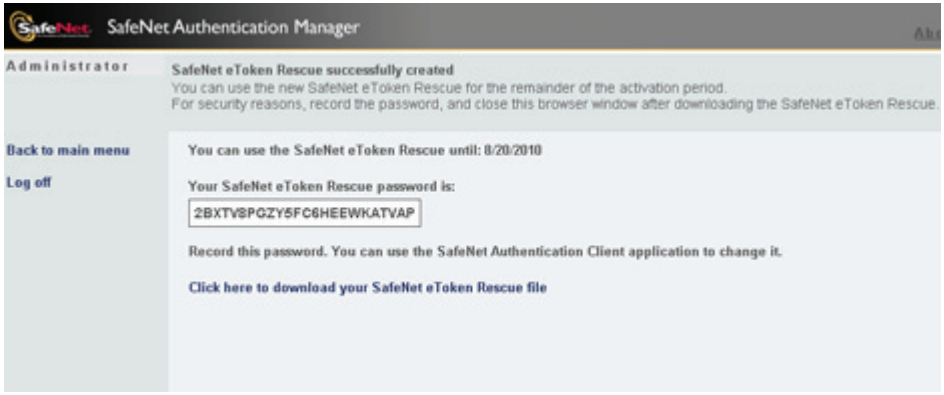
Note:
If access to your SafeNet eToken Rescue was already enabled, the expiration date remains the date that was set when it was first activated.

To replace your SafeNet eToken Rescue file:

1. In the *Welcome to the Rescue Service Center* window, select **Replace a lost SafeNet eToken Rescue.**

   The following information is displayed:

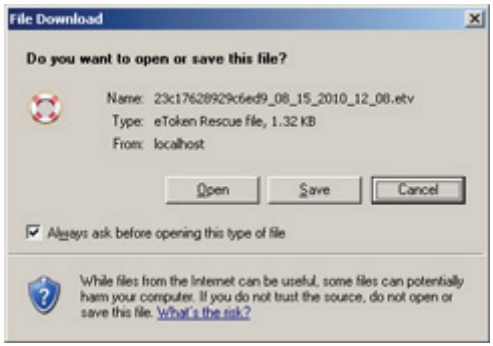
   - a *SafeNet eToken Rescue successfully created* message
   - the SafeNet eToken Rescue expiration date
   - the new SafeNet eToken Rescue password



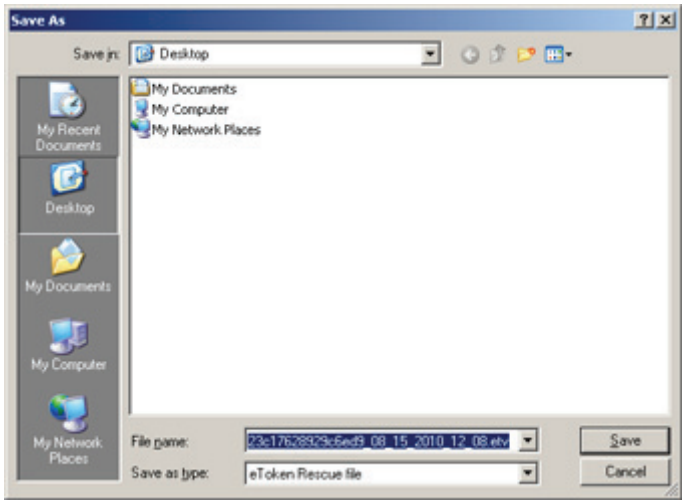
2. Write down the SafeNet eToken Rescue password, and save it in a safe place.

   Tip:
   It is your responsibility to remember your new SafeNet eToken Rescue password. You may need to provide it to gain access to your SafeNet eToken Rescue content.

3. Click the link **Click here to download your SafeNet eToken Rescue file**.
   The *File Download* window opens.

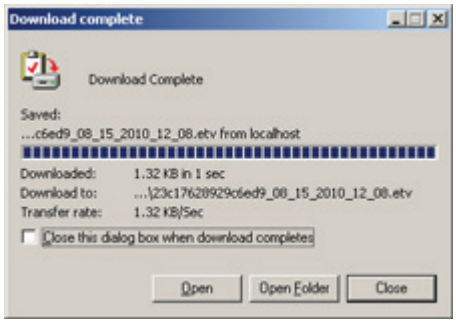


4. Click **Save**.
   The *Save As* window opens.

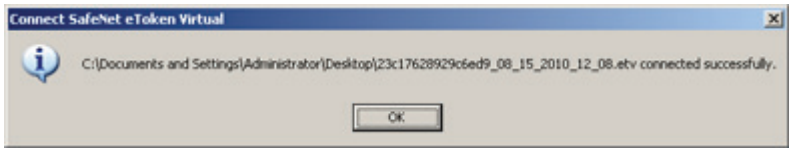


5. Select a location on your computer or external device to store the SafeNet eToken Rescue, and click **Save**.

The *Download Complete* window opens.



6. Click **Open** to define the file to SafeNet Authentication Client.



7. Click **OK** to close the dialog box.

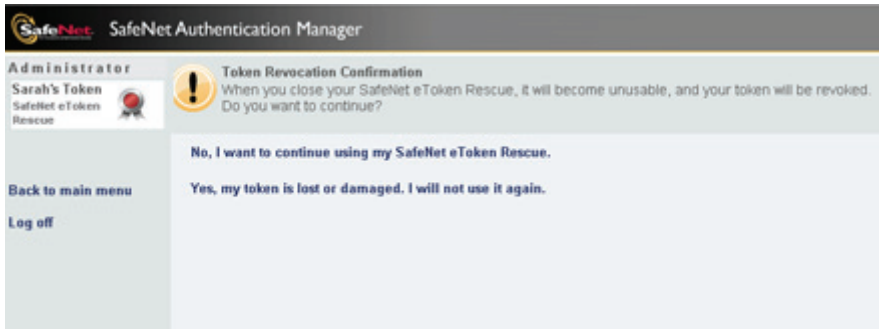
The replacement SafeNet eToken Rescue is saved to your computer or external device.

Closing Your SafeNet eToken Rescue

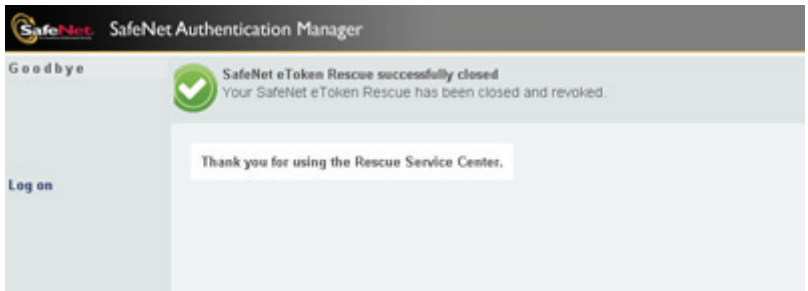
For security reasons, close your activated SafeNet eToken Rescue when you no longer need it. A SafeNet eToken Rescue can never be used again after it is closed.

To close your SafeNet eToken Rescue:

1. In the *Welcome to the Rescue Service Center* window, select **Close the SafeNet eToken Rescue**.
   The *Token Revocation Confirmation* window opens.



2. Select **Yes, my token is lost or damaged. I will not use it again.**
   A *SafeNet eToken Rescue successfully closed* message is displayed.



   The SafeNet eToken Rescue is closed and can never be used again.

Part IV SAM Agent

The following chapter describes how to use SafeNet Authentication Client's *SAM Agent*.

In this section:

- Chapter 10: SAM Agent (page 141)

Chapter 10

SAM Agent

The SafeNet Authentication Client includes the *SAM Agent* facility.

In this chapter:

- SAM Agent Overview
- Viewing the SAM Agent Status
- Verifying Your Token Content
- Downloading a SafeNet eToken Rescue

SAM Agent Overview

Depending on your SafeNet Authentication Manager configuration, the *SAM Agent* facility does the following:

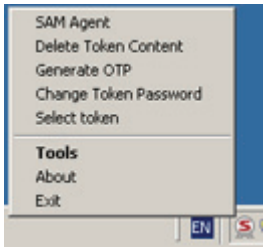
- Sends alerts to users when their token content is about to expire or is not up-to-date
- Enables SafeNet eToken Rescue file downloads
- Contributes token connection data to produce an Hourly Distribution of Token Connections report for your administrator

Viewing the SAM Agent Status

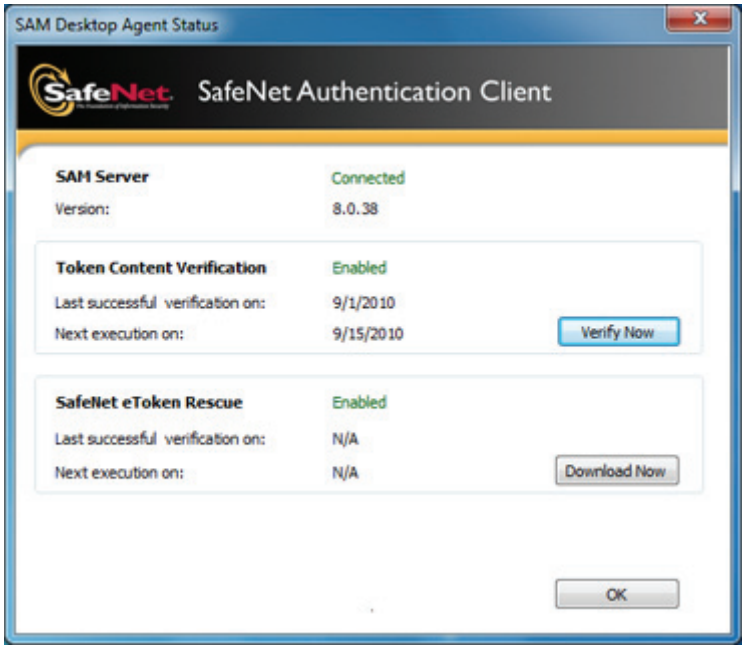
View the SAM Agent status from the *SafeNet Authentication Client* tray menu.

To view the SAM Agent status:

- Right-click the *SafeNet Authentication Client* tray icon, and from the menu, select **SAM Agent**.



The *SAM Desktop Agent Status* window opens.



The following information is displayed:

- SAM Server
  - Shows if the SAM Agent is connected to the SAM Server
  - Displays the SAM Agent version number
- Token Content Verification
  - Shows if the token content verification feature is enabled
  - Displays the date that the SAM Agent last checked if the token content needed updating
  - Displays the date of the next scheduled token content check
- SafeNet eToken Rescue
  - Shows if the SafeNet eToken Rescue verification feature is enabled
  - Displays the date that the SAM Agent last checked if the SafeNet eToken Rescue needed updating
  - Displays the date of the next scheduled SafeNet eToken Rescue check

Verifying Your Token Content

During the following events, the system checks if the token content on your connected token needs to be updated:

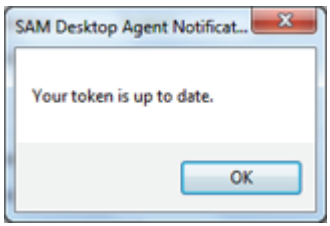
- You access the Self Service Center
- The SAM Agent performs a scheduled check
- Depending on your SafeNet Authentication Manager configuration, you can use the SAM Agent to verify your token content

If your token content is found to be out-of-date, a message is displayed.

When your token content needs to be updated, we recommend using the Self Service Center to update it as soon as possible.

To verify your token content:

1. Open the *SAM Desktop Agent Status* window.
   For more information, see *Viewing the SAM Agent Status* on page 142.
2. Click **Verify Now**.
   The SAM Agent checks if your token content needs to be updated, and a message is displayed.



3. If a message is displayed that your token content needs to be updated, use the Self Service Center to update it.

Downloading a SafeNet eToken Rescue

You can save your token content to a *SafeNet eToken Rescue*, a secure backup file on your computer or external device. A SafeNet eToken Rescue is a SafeNet eToken Virtual product that can be activated for use as a temporary token replacement if your token is lost or damaged.

Ensure that you have an updated SafeNet eToken Rescue file each time you leave on a trip so that the most up-to-date token content is backed up and available to you.

If your token is lost or damaged when you are away from your office, contact your administrator, or use the Rescue Service Center to report your lost token and to activate your SafeNet eToken Rescue. Then use your SafeNet eToken Rescue as you would use your physical token.

Note:
A SafeNet eToken Rescue is accessible for a limited time only, and only through a password that is disclosed when you report your token as lost or damaged to your administrator or to the Rescue Service Center.

Depending on your SafeNet Authentication Manager configuration, you can use the SAM Agent to verify that you have an up-to-date SafeNet eToken Rescue. If it is not up-to-date, you can manually download an updated SafeNet eToken Rescue.

To verify your SafeNet eToken Rescue, and download an updated one:

1. Open the *SAM Agent Status* window.
   For more information, see *Viewing the SAM Agent Status* on page 142.
2. Click **Download Now**.
3. A new SafeNet eToken Rescue file is downloaded, and a message is displayed.