

## Expiring Token replacement process summary



Author:	Seb Mills
Version:	1.0
Status:	Public
Date:	25-Jul-2008
Classification:	Public

## Contents

Contents .....	2
Introduction .....	3
Summary of the replacement process .....	4
Key steps .....	4
User experience .....	4
Costs .....	4
Expiring token replacement timeline .....	5

## Introduction

All RSA SecurID tokens, as supplied as part of the SecurID from Signify authentication service, have an expiry date. This date is built-in to the token at the point of manufacture by RSA and indicates the point in time when it will cease to display tokencodes. The expiry date can be seen on the reverse of the token etched into the casing (MM/DD/YY). When the token expires, the word "OFF" shows on the display or the display will be blank.



Signify's Identity Management Centre (IMC) and provisioning services provide a simple and efficient way to manage the process of replacing expiring tokens to provide seamless continuity of service to your end users. This document describes that process.

The process is designed to be clear and easy for:

- End users to indicate how they'd like the replacement token delivered to them
- Administrators to be able to see at any time how the process for replacing end user's tokens is proceeding, and manage the process of capturing the most useful replacement shipping address from those end users.

Signify will perform the physical shipment of replacement tokens directly to your end users, removing the need for you to deal with this.

The customer administrators (HR Admin) can maintain full control and visibility of the replacement process, so that they know when tokens are being replaced, to whom, and to where. This information can be viewed by clicking on the 'Expiring Tokens' link from My IMC (<https://imc.signify.net/myimc/admin/tokens/expiring-list.asp>)

## Summary of the replacement process

### Key steps

The expiry process includes the following key steps. A detailed timeline is described later.

1. Approximately 8 weeks before tokens expire, HR Administrators at the customer are notified that they have some tokens that are due to expire, and the date on which they expire. The administrators are then given the chance to:
  - a. indicate where they want the replacement token to be sent. e.g. if they know that the user is based in a certain office, or they know what address the token should be sent to
  - b. indicate that the token shouldn't be replaced
  - c. or indicate that they would like the end user themselves to confirm what address the token should be sent to
2. A few weeks later, end users will be e-mailed to let them know that their token is due to expire, and allow them to correct their delivery address.
3. 30 days before expiry date, Signify will start sending tokens that have a delivery address confirmed directly to the end users. Users are still able to confirm their replacement address during the next 20 days.
4. 10 days before the tokens expire, replacements for any unassigned tokens and tokens for users whose address have not been confirmed will be moved to your token pool and shipped to a relevant Administrator.

### User experience

Once the user receives their new token, they can start using the token straight away. There is no need to change PIN as it is carried over from the expiring token. Once they have logged in with their new token the old one is immediately disabled and can be discarded or sent to Signify for environmental disposal.

### Costs

The cost of your organisation's replacement tokens are added to the renewal statement that relates to the service period for which the tokens are due to expire. As the service is renewed in advance any expiring tokens should have been covered well before they expire.

## Expiring token replacement timeline

The table below shows the timeline that different events will occur during the process.

Days From Expiry	Action
90	Expiring token process starts. Administrators have full visibility of the tokens and users affected. Any tokens due to expire within this period are treated as expiring instead of the reported reason by the user.
60	Administrators receive summary of expiring tokens and are invited to confirm replacement addresses or request the token not to be replaced
59-45	Administrators confirm replacement addresses for users with shared addresses
45	End users with private or unconfirmed addresses asked to confirm replacement address
44-35	End users confirm replacement address
35	Reminder sent to users with unconfirmed addresses.
31	End users with confirmed addresses informed that replacement token will ship soon.
30	Shipping starts for users with confirmed addresses, administrators receive shipping summary when all tokens have been shipped.
29-10	Users receive replacement tokens. Users continue to confirm replacement addresses and new tokens shipped daily.
10	Tokens for users without confirmed address are shipped to administrator and administrators receive final summary
0	Tokens expire