

# **Setting your Signify Security Policy**

Author: Dave Abraham  
Version: 1



## Contents

Contents.....	2
Introduction .....	3
Organisation Policy Settings .....	4
One Policy across the whole organisation?.....	4
Allocation of Admin Roles.....	5
Who will be requesting New Users? .....	5
Who will be provisioning New Users? .....	5
Who will be revoking user accounts?.....	6
Security Policy Settings.....	6
What types of Authentication Credential are permitted for your users .....	7
One-Time Passcode Options.....	7
Helpdesk Options .....	7
Automatic Device selection on helpdesk pages.....	8
Alternative Authentication Options .....	8
Security Questions.....	9
Confirm access to an e-mail address.....	9
Confirm possession of mobile phone.....	9
Confirm identity via a Notary.....	10
Forgotten PIN/Password Options .....	10
Lost/Broken Token/Smartcard Options .....	10
Emergency Access Options.....	11
Summary.....	11



## Introduction

Signify's Managed Authentication Services allow you to implement a range of authentication technologies to your organisation's network.

Many of these technologies allow you to increase your level of authentication, based upon industry leading strong authentication technologies, using a physical token for authentication, whether that token is an RSA SecurID device, a mobile phone, a smartcard or another token device.

However whether you implement one of these technologies using Signify's managed services, or by running your own servers to host these technologies, however technically secure the technology is, the security of your network is only as good as the processes and procedures that you put in place to control the roll out, replacement, and revocation of users. The set of processes and procedures that you put in place is your *policy*.

If implementing one or more technologies yourself, you will need to plan:

- which technologies you want to implement
- how you are going to roll out the users, and what logistics will be necessary
- how you will train the users
- what policies and procedures you will put in place to authenticate users if they need to replace one of their credentials, be that a forgotten PIN or password, a lost or broken token or smartcard etc.
- the logistics for sending out replacement credentials
- what you will do with users who need to log in whilst they are waiting for a replacement physical device to be sent to them.

Each decision can affect the security, cost, implementation time, ease of use, and internal resource requirements of your implementation.

Signify has made these decisions and implementations straightforward for you. We have a standard range of options for each of the above decisions that you can make. All your options can be managed via the Identity Management Centre (IMC) by changing your Organisational Profile and your Security Policy, and can be changed whenever you wish via the IMC, any changes being automatically reflected throughout Signify's service, including fulfilment, user administration, and helpdesk services.

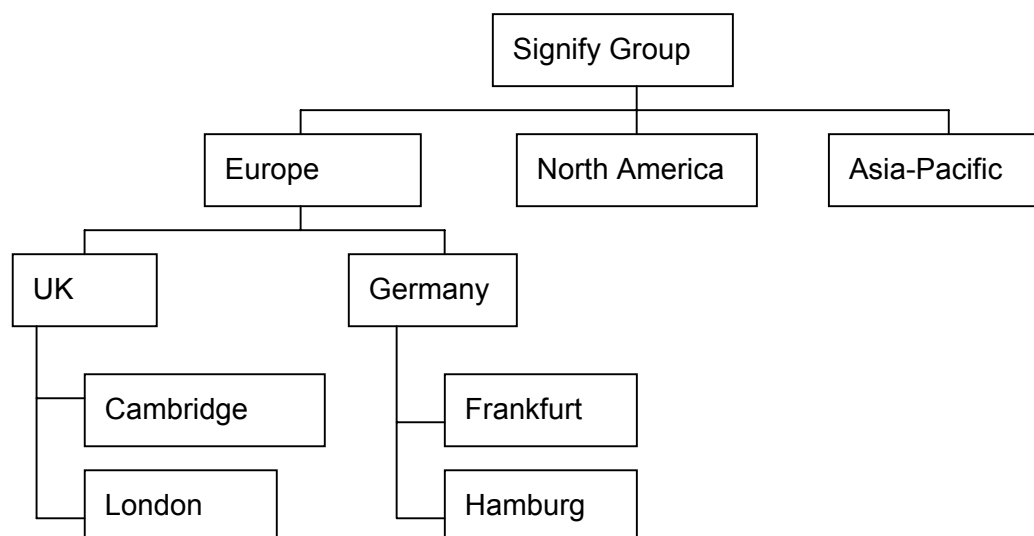
This document discusses many of those options, to help you understand how to customise the Signify service to meet your organisation's requirements. It should provide a basis for a security policy planning meeting either within your organisation, or with Signify.



## Organisation Policy Settings

### One Policy across the whole organisation?

An organisation can be modelled on the IMC as a hierarchical collection of sub-organisations. This is normally done on a geographical basis, e.g.:



You could of course, in the example above, further break down the Cambridge office, for example, into a number of business units, or departments. Alternatively you may model your organisation along business units first, and then geographically further down the tree.

This can allow you to delegate administration of individual groups of users to an individual location, or to a set of locations, or within a functional business unit.

You can have administrators assigned to any point in the hierarchy, and they can have *scope* either just for the specific organisation that they are allocated to, or to all sub-organisations below it in the hierarchy, or both.

You can store pools of tokens at each site, or at strategically selected sites.

It is normally recommended to have a single security policy across the whole organisation. However if appropriate you can set different security policies for separate organisations or trees of organisations. For example you may want one organisational unit to be required to have RSA SecurID tokens, whereas another unit may be allowed to have SMS passcodes as well as SecurID.



## Allocation of Admin Roles

There is a range of admin roles. See the Administrator Guide for the description of each role. These roles allow the division of the roles and responsibilities to be allocated throughout your organisation as appropriate. It is recommended that there are always at least 2 Security Officers at the top-level organisation, since the Security Officers are the ones able to set the security policy, and allocate who the other individual administrators are.

The other admin roles can be kept centrally, or specific roles delegated to staff with appropriate authority for their individual business areas.

The IMC enforces the scope over which an administrator can perform their tasks, and controls what tasks they can perform. Additionally, a full audit trail is kept of each action and who performed it, backed up by strong authentication. Therefore you can delegate tasks whilst maintaining full control and visibility of your processes.

Three key decisions that need to be made are who will be requesting new users, who will be allocating credentials to those users (especially if a physical token is involved), and who will be revoking users when they are no longer allowed access to your systems.

### Who will be requesting New Users?

The first step of setting up a new user is for an 'HR Admin' to enter the details into the IMC. The term 'HR' is used because it is someone responsible for people – this admin role can sit within the HR department, in the IT department, or for example in a sales department if the users being set up are customers.

A new user is usually requested by an HR Admin filling in a form on the IMC to give the details of the requested user, but it can be performed by an automated bulk import, where the HR Admin then simply approves all the new users that have been imported.

The user is not actually provisioned at this point.

You should decide who are the most appropriate people within an organisation, that they can input the details, so that you don't have one person send another person an e-mail saying 'Please set up this user' (where an e-mail can easily be spoofed to generate a non-genuine request) – the first user simply enters the details directly into the IMC.

### Who will be provisioning New Users?

Once a user has been requested, their credentials can be allocated to them. A 'Fulfilment Operator' performs this task. Someone working in an office where the new user works, who has a local pool of tokens, can do this and they can allocate a



token from their stock. Alternatively it could be a central resource, maybe the IT department, or maybe the mailroom. Alternatively it could be Signify, who can provide the fulfilment services to ship the packages directly to your end users, anywhere in the country or the world, using the appropriate delivery method, which can mean that if you have remote home workers you can have an HR Admin request a new user, and not have to worry about any logistics yourself.

So the requesting of users, and the subsequent provisioning can be completely separated. Alternatively, if you wish, one person can take both HR Admin and Fulfilment Operator roles, and roll out users themselves.

### **Who will be revoking user accounts?**

One of the key processes to maintaining an organisation's security is the revocation of users when they should no longer have access. Many organisations find that the IT department only finds out long after users have left that their accounts should have been removed. This especially crucial where the access being provided by those accounts is for remote access into the organisation's network. Imagine a user leaving and still having a valid password or SecurID token that can be used to log into the VPN.

The IMC allows the revocation of user accounts to be delegated to appropriate departments that do know when users leave – whether that be the HR department or the payroll department for example. The appropriate administrator has a simple web interface to revoke users (whether they have returned their credentials or not), without needing to rely on the IT department to perform any tasks.

## **Security Policy Settings**

The security policy defines what types of credentials are permitted in your organisation (or in each sub-organisation), and also defines a set of helpdesk processes to ensure that your organisation's security is maintained throughout the lifecycle of each user. It is a fact of life that users will occasionally lose or break devices, forget their passwords and PINs etc. Signify have focussed on making sure that the IMC enables these situations to be dealt with:

- as a matter of standard daily business for the organisation, with minimal cost to the organisation
- easily and efficiently for the end user
- whilst maintaining the security of the organisation to the level that the organisation wishes to achieve

The following sections describe the settings that you can set in the security policy.



## **What types of Authentication Credential are permitted for your users**

You can set what types of authentication credential are allowed for your users. Only the options that you tick will be made available to your HR Admins when they request a new users.

### **One-Time Passcode Options**

If you have enabled any One-Time Passcode authentication credentials (SMS, or E-mail OTP), then you will be given a set of options as to the level of security enforced with those credentials. This includes whether e-mail, SMS or both are permitted for the delivery of the one-time passcodes, and whether the authentication should use simple or strong PIN mode.

In Simple PIN Mode, the user requests a passcode, and is asked to enter their PIN at that point. If they get their PIN right, their passcode is sent to them, and then to log in, the user simply has to enter the passcode that they receive in the SMS or in their e-mail.

In Strong PIN Mode, the user requests the passcode as above, and enters their PIN. However when they then receive their passcode, when they log in, they have to enter their PIN, followed by the passcode that they received. This is slightly more cumbersome, as the user ends up having to enter their PIN twice, but offers increased security because even if the passcode were snooped as it crossed the SMS or e-mail networks, it couldn't be used by the snooper without the PIN. This is the classic security trade-off between security and convenience.

However for most organisations, Simple PIN Mode is appropriate – if the higher level of security is required, this is often best achieved by using RSA SecurID, with a higher cost, but a more convenient end user experience.

### **Helpdesk Options**

Most of the security policy options apply to the end-user helpdesk. This is because most vulnerability in an organisation's security with regard to user authentication is in its processes regarding helpdesk calls. For example, if a user can phone up a helpdesk and say that they have lost their token, unless the helpdesk makes sure who the person is before sending out a replacement, then they could just be sending out a token someone that shouldn't be given access. You can have the greatest security technology in the world, but if you give the keys to the wrong person then they can walk straight through it.

The security policy allows you to adjust your security stance between maximum security and ease of use for your end users (and for your helpdesk staff – for example if you've traditionally had a fairly lax approach, you may not want to jump to



an overly sensitive security stance, which could come across as customer unfriendly, or even downright unhelpful. With the IMC you can phase in increases in security)

### **Automatic Device selection on helpdesk pages**

When a user accesses the helpdesk, they are first asked to indicate who they are. This is then used to provide the most relevant help to the user. The helpdesk can then also look up what authentication credentials are used by this user to further improve the relevance of the helpdesk. This optional feature is known as 'login assistance'. However if you employ a number of different credentials within your userbase from passwords through to SecurID, an attacker could use login assistance to identify which users have the weaker forms of authentication. It is therefore recommended that login assistance is only enabled if all your users have strong authentication, ideally all of the same type.

### **Alternative Authentication Options**

Many helpdesk operations require the user to identify themselves before that operation can be completed. Most of these actions involve replacing one or more of their credentials, e.g. their PIN, password or token. As such, they clearly don't have all their credentials, and therefore we can't ask them to log into the IMC, where we could then perform an authenticated session.

Therefore the IMC has a range of methods that can be used to identify the person in the absence of their credentials. These methods, we call 'Alternative Authentication' (Alt Auth). The IMC supports 4 AltAuth methods to identify the user:

- Confirming that they know the answers to some security questions that they have set themselves
- Confirming that they have access to one of their registered e-mail addresses
- Confirming that they have their mobile phone with them
- Confirming their identity with a trusted person within the organisation, a 'Notary'

Within the security policy you can define which or all of those methods are available to identify a user, and how many of those must be used. For example to increase your level of security, you could increase the number of security questions people are asked, or you could insist that they complete 2 or 3 of the Alt Auth methods, rather than just one. This will considerably increase security, but will be harder to use for the end user – if they either don't have access to their e-mail account etc or haven't registered their mobile phone number with the IMC.



The IMC's helpdesk functionality provides a full audit of the whole helpdesk process so that the authentication of the user and subsequent replacement of a credential is auditable and traceable.

The sections below describe each Alt Auth method in turn.

## **Security Questions**

The security questions are a very flexible method of varying the level of security. They are the most flexible option for end users, since if they have set good questions, then they can be quite secure, but can be used from anywhere. Within the security policy you can set how many questions the user must set up during registration (the more they set up, the harder it will be for an attacker to research the questions), but it may result in less secure questions – a user may for example struggle to set up more than 3 good questions that they can actually remember the answer to several months later.

You can set up how many questions the user will get asked, and how many they will have to get right – for example they may have to have 3 questions set, get asked all 3, but only have to get 2 of them right. Or it may be that you ask them 2 of their 3 questions, and have to get both correct. When the user is asked the questions, they are asked for one letter of the answer.

Finally you can set how many times you want the user to be able to attempt the answer before stopping them, to avoid a trial and error attack against the questions.

## **Confirm access to an e-mail address**

This is a very convenient method of identifying a person when they are in the office and have for example forgotten their PIN or lost their token. If they are sat at their desk, they can simply have an e-mail sent to them, which will contain a unique link which they can click on to prove that they have access to their e-mail. The one downside is that if the person is not in the office, and has not registered any additional e-mail addresses, then if they need to use their Signify credentials to access their e-mail, they won't be able to use this method. However each of the other 3 methods will still be available.

## **Confirm possession of mobile phone**

This method is similar to the e-mail confirmation, but in this case is ideal where the user is not in the office when they wish to perform their helpdesk action. The user is sent an SMS to their mobile phone, containing a unique reference code. The user can then enter that reference code into the helpdesk (or tell it to a telephone helpdesk operator), to prove that they have their mobile phone with them.

The user must have their mobile phone registered on the IMC before they need to call on the helpdesk though.



## **Confirm identity via a Notary**

The final AltAuth method is referred to as Notary authentication. This is where the user asks for a trusted person to confirm their identity. If the user requests Notary authentication, then an e-mail is sent to all the notaries who have 'scope' over that user. One of the notaries can then pick up that action, and contact the user, to confirm 2 things – one that they recognise their voice, or are able to identify them in some other way, and secondly by confirming that they have really requested the helpdesk action (for example, there's no point phoning up confirming that Joe Bloggs is Joe Bloggs if you don't also ask if he contacted the helpdesk 5 minutes ago about having lost their token).

Once the notary has confirmed the identity and authenticity of the request, they can then approve it on the IMC, and there will be an audit log entry identifying that notary as having performed that step.

Notary authentication is not made immediately available to end users, so as to ensure that notaries are not unduly bothered by user requests when an alternative method would be equally good. Thus Notaries are only made available after the end user has failed to get their security questions right.

## **Forgotten PIN/Password Options**

The level of authentication for a forgotten PIN or Password can be set differently to that for replacing a physical device. However they are normally set to the same level. The default on the medium security level is to require one of the Alt Auth methods. If the user completes the required number of methods, then they will be able to reset their PIN/password there and then, or have an e-mail sent to them so that they can set it at a later date.

## **Lost/Broken Token/Smartcard Options**

As for forgotten PIN, the default medium security setting for reporting a token lost or broken is any one of the four AltAuth methods. After this AltAuth is completed, the user will be able to disable the token. They will then be able to indicate where the replacement token should be sent. You can set the security policy to restrict them to only their registered addresses (which will include all your office addresses), to only their primary address that is registered directly to them, or to allow them to enter any address where they would like the token sent to. Obviously the last option is the least secure, and therefore is not enabled by default, but it is the most convenient if you have users that regularly travel around. Another classic security/convenience trade-off.



## Emergency Access Options

Once a user has registered a physical token as lost or broken, they obviously cannot gain access to your systems until they get a replacement. Where Signify are responsible for sending out replacements for your organisation, the replacement will normally be sent out the same day that it is requested, and always within 12 working hours. However obviously this can mean that the user is unable to work remotely for at least a day, and sometimes longer, especially if the user is travelling abroad at the time. This is the correct thing that should happen for an organisation that wants maximum security.

However again, a trade-off can be made between ultimate security, and convenience and productivity. Signify therefore makes available a feature called 'Emergency Access'. For maximum security, this can be disabled, but most customers find the benefits of increased flexibility, especially with its secure implementation that it is well worth having enabled.

Once the user has registered their token as requiring replacement, and has requested a replacement, if your security policy enables the user to have emergency access, then they will be offered the choice as to whether they wish to enable it. If they do, they may be asked to complete some additional AltAuth methods (depending upon your security policy), and then will be provided with a set of "One-Time Passcodes". This is a set of passcodes, just like the ones that display on a SecurID token, or get sent to a mobile phone in the case of the SMS Passcode service. These One-Time Passcodes can be printed from the screen, e-mailed to the user or sent to the user by SMS. The user can then use each one in turn when they want to log in. However the passcode is *only* to replace the token – they still have to use their PIN before it, just like with a token, therefore they have to know their PIN.

Therefore in your security policy, you have to indicate whether you want to enable emergency access, and if you do, how you want to authenticate the person. You can just leave the AltAuth methods as being the same as to report a broken/lost token, in which case the user can step through to emergency access immediately.

Alternatively you may say that 1 method is enough to request the replacement, but you must complete 2 methods to obtain emergency access, which provides an extra step of security before enabling this access.

## Summary

This discussion should have given you an overview of all the flexibility that can be applied to run your authentication system to the level of security, and convenience to meet your organisation's requirements.

This document should help you to decide what is the best policy for you, and is ideally used as a preparation for a security planning meeting with Signify, so that the



options can be discussed based upon a knowledge of the options, and the policy set on the IMC to ensure that Signify delivers a service that meets your requirements.