

Signify Administrator Guide



Author:	Dave Abraham
Version:	3.8
Status:	Published
Date:	8-Feb-2008
Classification:	Public

Contents

Contents	2
Introduction	3
Identity Management Centre (IMC)	5
Overview	5
My IMC – your portal into the IMC.....	5
Advanced Administration – advanced interface to IMC	5
Organisations	6
Shared Addresses and Phone Numbers	6
Scope.....	6
Overview of Administrative Roles	6
Security Officer	7
HR Admin	8
Tech Admin	8
Optional Roles	8
Fulfilment Operator	8
Helpdesk Operator.....	8
Notary	9
Fulfilment Admin	9
How to perform common actions	10
Adding a New User	11
Request a New RSA SecurID User to be shipped by Signify	12
Request a New RSA SecurID User if you will perform Fulfilment within your Organisation.....	13
Request a New User from a local fulfilment pool	13
Fulfilling a new user from a local fulfilment pool	13
Set up a New Passcode OnDemand User	14
Re-allocate a token from one user to another.....	15
Allocating an RSA SecurID token or Passcode OnDemand device to a user that has previously had a token and registered	15
Performing Actions on Existing Users	16
Revoking a user	16
Activating a user on an Authentication Node	16
Removing access to an Authentication Node for a user	18
Changing the username of a user for an Auth Node	18
Authentication Nodes	19

Set up a new Authentication Node	19
Changing the IP address of an Authentication Node	20
Security Officer Tasks	22
Allocate Administrative Roles.....	22
Set an organisation's security level	22
Obtaining Logs and Alerts	23
View Logs	23
View fulfilment status	24
Other Tasks.....	24
Receiving a batch of token packs and rolling them out to users	24
Managing Organisations – sub-organisations and customers	25
Glossary	26

Introduction

Signify's Identity Management Services deliver fully managed systems to provide the lifecycle of identity management for your users.

This Admin Guide provides guidance to administrators on version 3 of the IMC. For customers with a basic configuration, there is a Quick Admin guide, taking them through the most common functions.

This lifecycle comprises the secure, auditable management of a range of processes including:

- Setting up new users
- Assignment of authentication devices and credentials
- Registration of users with corresponding credentials
- Authenticating users as they log into your various computer systems (authentication nodes)
- Managing the process of the replacement of the user's authentication credentials if lost or forgotten
- Alerting appropriate individuals when specified events occur or actions are pending
- Removing user's access rights to authentication nodes when appropriate
- Deleting the user

Signify has automated and implemented a range of procedures to meet our client's working practices. In most cases your requirements can be met by choosing the right combination of standard procedures. The full range of Identity Lifecycle procedures and how the IMC makes them available to you, entitled 'Signify's Modular Architecture for delivering Secure Identity Management', is available on request..

A number of different people within your organisation can perform these procedures, for example, requesting a new user. These administrators can simply access the IMC using a standard web browser to make changes and most changes requested will then automatically be applied, or start a process.

The administrative functions available to each administrator are defined by 'admin roles'. This document will summarise these admin roles, and guide you as an administrator, through what you can do, and how to do it.

Identity Management Centre (IMC)

Overview

The Signify Identity Management Centre (IMC) is your interface with Signify's services. You can use this to manage almost every aspect of your managed service. Within the IMC there are sets of Objects that can be managed, and Administrative Roles, which give users the permissions to be able to operate on those objects.

Some of the objects that you will deal with include:

- People
- Organisations
- Authentication Nodes (authnodes)
- Authentication Credentials, including Authentication Devices
- Addresses, telephone numbers and e-mail addresses

The IMC stores relationships between these various objects. If you are an Administrator, then you may have permission to read, create, edit, and delete some of these types of objects, and to modify relationships between objects.

My IMC – your portal into the IMC

As both an end-user and as an administrator, your first port of call is always the My IMC area of Signify's web site. You can get here by visiting www.signify.net and logging in.

You will then enter the My IMC area, which will automatically display the links appropriate to your administrative roles.

These links will be displayed on the left-hand side of the window, with useful summary information relevant to you in the rest of the screen. Most of the links on the left-hand side will take you to wizards that will simply step you through the required process. You can also go to Advanced Administration area of the IMC that provides many more functions.

You can always get back to this page quickly by going to www.signify.net/myimc or by clicking on a link to My IMC.

Advanced Administration – advanced interface to IMC

You will be able to perform most common actions by using the My IMC portal page as described above. The Advanced Administration section allows you to work more directly on individual objects such as Users, Organisations, Authnodes and Tokens, and also to access logs of your user's activity.

Organisations

Within the IMC, the largest unit of sub-division is the 'Organisation'. Your organisation is initially created on the IMC as a single Organisation, with associated addresses (for each office location) with corresponding phone numbers, plus a Security policy and specified administrators.

You can create 'Sub-organisations' if you choose to have separate Security Policies for separate parts of your organisation, or if you wish to have different administrators able to manage different parts of your user base.

You can also create 'Customer' organisations, again with a separate Security Policy and administrators if required.

Who can see what when you have multiple related organisations is defined by an administrator's scope – see below.

Shared Addresses and Phone Numbers

Each organisation has one or more addresses associated with it, e.g. one for each of its offices, and similarly a phone number.

When you request a new user, you can let the user be automatically allocated these addresses. In this way, if the organisation's address moves, then you only need to edit the organisation's address, and then each user related that has that 'shared address' will have their contact details automatically updated.

Scope

Admin roles have a 'scope' associated with them, such that an administrator can only operate on items within their scope. In essence, a user will only see objects that they are able to work on.

For example, you may be an HR Admin for an Organisation. You will be able to request new users for that organisation. You will also be able to choose which Authentication Nodes and the type of Authentication Devices that person will use. If you are also an HR Admin for a second organisation, when you request a user, you will be able to choose which of those two organisations you would like to add that user for.

The scope of an Admin role can apply either just to an organisation, just to sub-organisations of the selected organisation, or to both. If you choose to apply the admin role to sub-organisations (and customers) then this cascades to all sub-organisations.

It should be noted that if you have a large organisation modelled on the IMC as a number of sub-organisations, not all users will see the same objects, dependent upon the scope that you have defined for each user.

Overview of Administrative Roles

The administration of your Signify service is managed by a number of administrative roles.

Each admin role should be assigned to at least one individual, however the same individual may be assigned multiple admin roles.

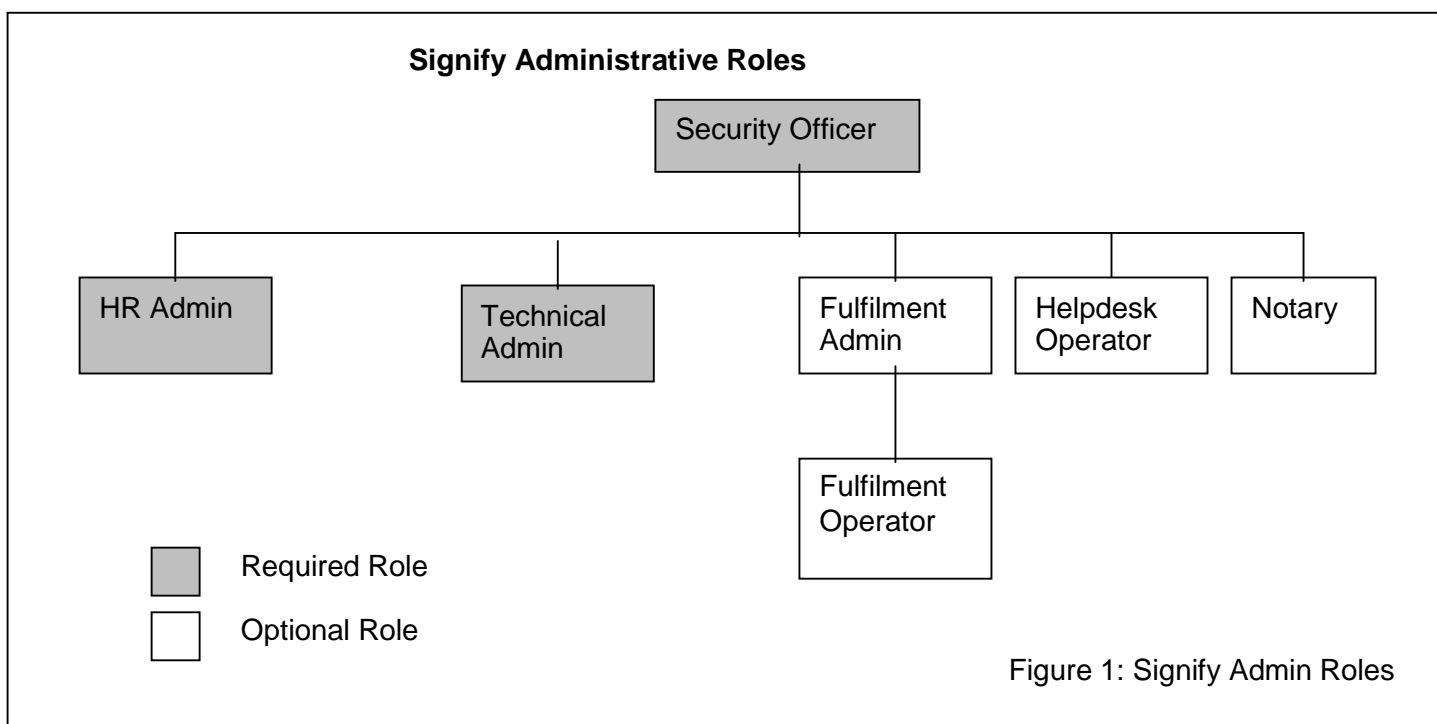
Thus it is possible in a small organisation for one person to hold all the admin roles required, and perform all the actions themselves. Conversely in a large organisation it is possible that each user can have only a single role, so that any attempt at fraudulent issuance of credentials is not possible by a single individual.

There are two classes of administrator - Required and Optional. Each organisation must have at least one:

- Security Officer
- HR Admin
- Tech Admin

Some organisations that have certain requirements may also optionally have:

- Fulfilment Operator (and optionally Fulfilment Admin)
- Helpdesk Operator (and optionally Helpdesk Admin)
- Notary



Security Officer

The Security Officer(s) is the ultimate point of authority for managing the security of the Customer and such as:

- appointing and revoking the administrator roles described below to different End Users
- changing the specific privileges of each administrator

- defining and modifying the overall Security Policy which specifies how the Customer's organisation and its End Users are managed within the IMC

HR Admin

An HR Admin can perform user-related tasks such as:

- enter details of additional end users required
- request changes (edit, delete) to their End Users
- modify which authnodes users can access
- view authentication logs and analysis of those logs on a per user basis (this level of personal information is not available to the tech admin, unless they are also an HR Admin)
- edit their organisation's details, such as name, addresses and phone numbers

Tech Admin

A Tech Admin can perform authnode-related tasks such as:

- set up new authnodes
- request changes (add, edit, delete) to their authnodes
- modify which users can access an authnode
- access authentication logs for their authnode

Optional Roles

Some organisations may receive additional processes and services from Signify which require additional roles within the IMC including:

Fulfilment Operator

Where organisations wish to keep a stock of tokens on their own premises to give out to their local users themselves. In this case the organisation must have a Fulfilment Operator who can then allocate tokens from their local stock, to users that have been requested by an HR Admin.

Helpdesk Operator

Where organisations run their own helpdesk that their users call, and they also wish their users to call this same helpdesk for Signify related issues, Signify can make Signify's web-based helpdesk available to operators at the customer organisation, to perform all helpdesk related activity on users within their scope. The helpdesk will automatically step the operator through the appropriate security processes for the user that they are working from. For a user to be able to perform these helpdesk tasks, they need to be set up as a Helpdesk Operator.

Notary

Where organisations wish to give their staff 'Emergency Access' for when their users have, for example, lost their token, then one of the options for obtaining emergency access is for the user to contact a Notary, who can then enable emergency access for the user. Other administrators can act as Notaries, but where necessary an end user can be a Notary, without needing to have any other form of administrative access, e.g. the user's Personal Assistant.

Fulfilment Admin

Where an organisation uses local token pools to manage unallocated stock of tokens, a fulfilment operator can only perform allocation of tokens that are in a pool to a user that has been requested by an HR Admin.

A Fulfilment Administrator can manage the set of token pools for their organisation – creating new ones as necessary, and moving tokens between token pools.

How to perform common actions

This section will describe many of the actions that an Administrator can perform. Most of them are available from the My IMC page, which is your personalised Signify area and contains links and information appropriate to the Admin Roles that are allocated to you.

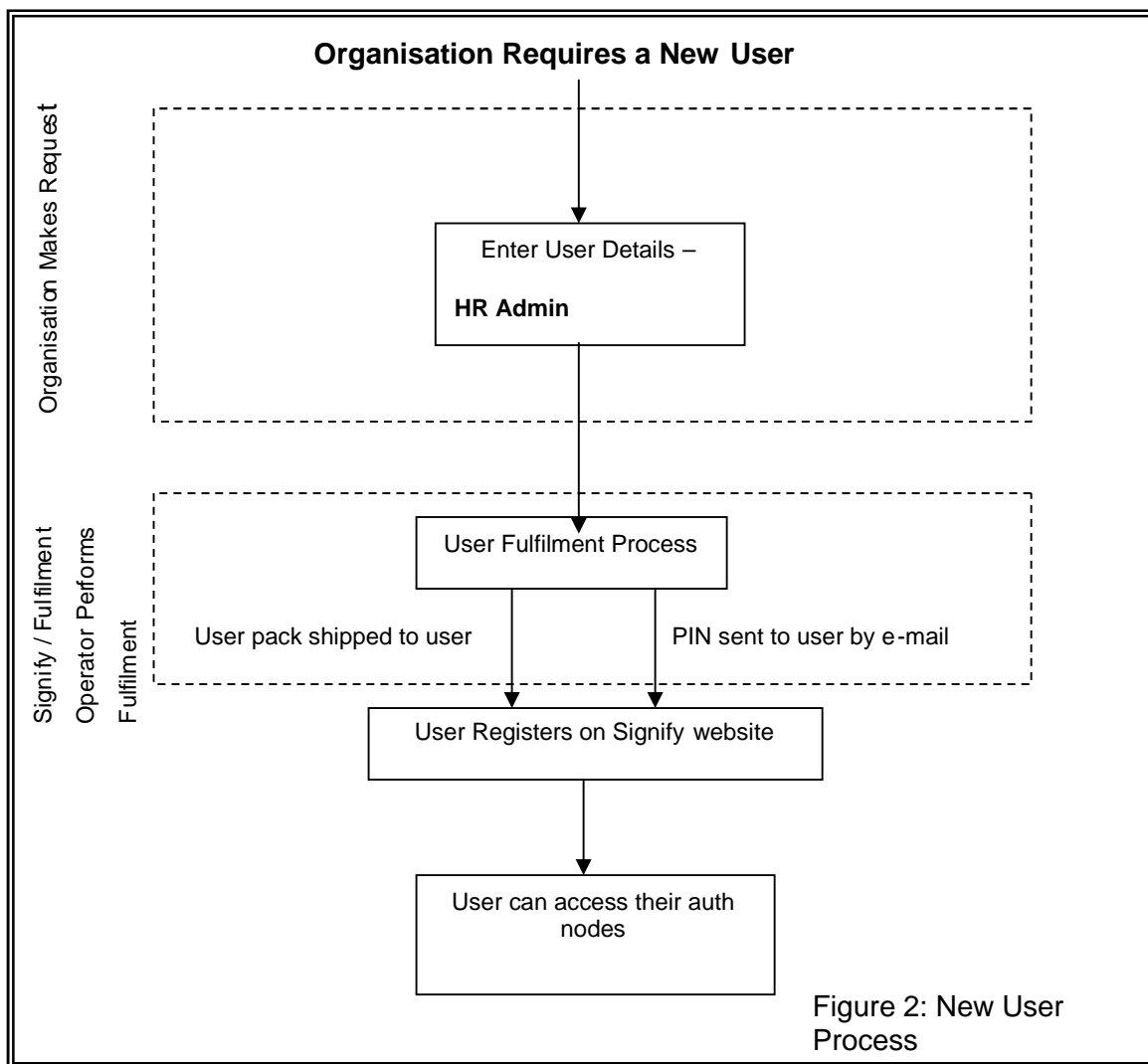
It is split into a number of sections, related to how you perform a complete process:

- Setting up a user and allocating a token
- Setting up new authnodes
- Security Officer tasks covering setting an Organisation's Security Policy and setting Administrator roles
- Obtaining and viewing logs

Adding a New User

When an organisation requires a new user, they can perform the whole process using the IMC. Each stage of the process is performed by a user who has been authenticated using Signify's Authentication Services, thereby providing a full audit trail of the issuance process.

An overview of the process is indicated below:



In summary, once an organisation decides that it requires one or more new users, it makes a request onto the IMC using a simple web form and enters the details of the user to be set up.

Once the user details have been entered, the Fulfilment process will proceed.

- If the request is for either a token to be sent to a user by Signify, or is for a Passcode OnDemand user, then the fulfilment process is handled by Signify automatically for you on the required date.
- In some organisations, for the fulfilment process, the user packs are held by the organisation ready for handing directly to users where they work in the same building, or for inclusion in a larger shipping process. This scenario is termed 'Local Fulfilment' and in this case the process is exactly the same as in Figure 1, except that the user pack shipment is performed by the organisation's Fulfilment Operator, rather than by Signify. The PIN is still automatically sent by Signify as in the diagram.

Request a New RSA SecurID User to be shipped by Signify

Admin level required: *HR Admin*

You can request a new user for any organisation for which you are an HR Admin. From your My IMC page, follow the link to **Request New User**. You will then be able to choose which organisation you wish to add the user for.

You will then be presented with a New User Request form. In this form, you should fill in the details of the new user that you wish to request.

The details required comprise:

- The person's name
- E-mail address – this is the address that their welcome e-mail will be sent
- Phone number – if this is a mobile number, then this can be used by the automated helpdesks to validate the user's identity during helpdesk processes
- Postal address – this is the address to which Signify will send the token, and is also the address that will be used to send replacement tokens to (though the end user can add additional addresses at a later point).
- In the Authentication Devices section, you should ensure that the Authentication Device is set to 'RSA SecurID'
- If you have stocks of tokens held by yourselves for 'local fulfilment' see the section entitled 'New User Requests with local fulfilment pools'. Otherwise ensure that the Token Pool is set to 'Signify fulfilment – RSA SecurID token'
- When you would like the token shipped to the user – this is the date when Signify will post the pack, not the date that it will be received. You should also choose the appropriate shipping method. If you choose Courier or Special Delivery, there will be an additional shipping charge, but the delivery of tokens is then insured and guaranteed by the relevant courier.

- Which Authentication nodes you would like them to be able to log into, and what username you require them to use on that Auth Node.

When complete, submit the form, using the button at the bottom. If you have additional users to add, simply click on the **Request New User** link, to repeat the process.

Note: Your organisation's security policy must have RSA SecurID enabled. If it is not enabled, ask your Security Officer to enable RSA SecurID for the organisation.

Request a New RSA SecurID User if you will perform Fulfilment within your Organisation

Request a New User from a local fulfilment pool

Admin Level Required: *HR Admin*

Your organisation may have elected to have 'Local Fulfilment Pools'. These are sets of user packs that your organisation keeps at its own location, and can give out to users rather than using Signify's fulfilment service. This is often useful if many of your staff are likely to be in the office or pass through the office at the time when you are setting them up. This may also be the case if you are delivering a service where you will be shipping items to your customer and you wish to put a Signify pack in with that package.

In this case, requesting a user is identical to that described in 'Request New User' in the section 'Token Pool' you should choose the appropriate pool from which you wish to allocate a token.

In this case, the Shipping Method and Shipping date are purely informational – it's up to your Fulfilment Operator (if it's a different person to the HR Admin), as to whether they use that information or not.

If you are also a fulfilment operator, you will then be able to allocate a token to that user – go to the section 'Fulfilling a new user from a local fulfilment pool'.

Note: Your organisation's security policy must have RSA SecurID enabled. If it is not enabled, ask your Security Officer to enable RSA SecurID for the organisation.

Fulfilling a new user from a local fulfilment pool

Admin Level Required: *Fulfilment Operator*

If there are new users that need to be fulfilled from one of your local pools of tokens, then in order to actually allocate a token to a person, you should follow the following procedure:

- Go to My IMC and choose '**User Fulfilment**'
- All the new user requests that have been made for your organisation will be listed, broken down by the status that they are in. Those that have been requested from one of your local token pools will have a 'Fulfil' button available to you in the action line. Choose which person you want to work on, and click the 'Fulfil' button.

- You will then be given the final step in the fulfilment process, the fulfilment pool will be the one selected by the requestor. You can then choose which token pack serial number to allocate to the user. You will probably want to get the pack from your stock, and once you know the serial number from that, enter that number on the screen).
- A new Welcome E-mail will be generated and automatically sent to the new user. By default, the Welcome e-mail will be sent immediately, which is ideal if you are handing the token directly to the person. However you can, if you wish, delay the sending of the e-mail – for example if you will be sending the token by post, you may wish to delay the e-mail a few hours so that it is delivered to the recipient overnight. If you wish to delay the sending of the e-mail, simply choose the delay from the drop down list.
- Finally click the **Ship Now** button

You should then hand over the token to the user, or pack and ship the token in whichever way that your internal procedures specify.

Set up a New Passcode OnDemand User

Admin level required: *HR Admin*

A Passcode OnDemand user will use their existing mobile phone or e-mail enabled device (e.g. Blackberry) as their authentication device. One-Time Passcodes will be sent to that device by SMS or e-mail when the user requests them. However users cannot setup their own device – the organisation must set up each device (so that you can ensure that only devices that you trust and authorise, can be used as credentials).

You can request a new user for any organisation for which you are an HR Admin. From your My IMC page, follow the link to **Request New User**. You will then be able to choose which company you wish to add the user for.

You will then be presented with a New User Request form. In this form, you should fill in the details of the new user that you wish to request.

The details required comprise:

- The person's name
- E-mail address – this is the address that their welcome e-mail will be sent
- Phone number
- Postal address
- In the 'Authentication Device Information' section, choose 'Passcode OnDemand Device' (If this option is not available, you will need to contact your security officer, see below).
- You should then choose (dependent upon the options in your Security policy) whether the device should be a mobile phone or e-mail device, the usability/security options for this device, and then the address of the device (either an e-mail address, or the international format of the phone number)
- Which authnodes you would like them to be able to log into, and what username you require them to use on that authnode.

When complete, submit the form, using the button at the bottom.

The user will then be set up immediately, automatically. A welcome e-mail will go directly to the e-mail address set up for the user (not the one for the Passcode OnDemand device), who will then be stepped through the registration process to enable their device.

If you have additional users to add, simply click on the **Request New User** link, to repeat the process.

Note: Your organisation's security policy must have the appropriate Security Policy settings enabled – this must include Passcode OnDemand device, and the appropriate options for Mobile phones and E-mail devices enabled. If it is not enabled, ask your Security Officer to enable RSA SecurID for the organisation.

Re-allocate a token from one user to another

Admin Level Required: *HR Admin and Fulfilment operator*

If you wish to revoke a SecurID token from one user, and re-allocate that token to a new user, there are 3 separate processes that are described in this document that you will need to follow::

- Follow the procedure 'Revoking a user'. When you do this, you should place the token into a local token pool, and indicate that you have the token yourself.
- Then follow the procedure for 'Request a New User from a local token pool'
- Then follow the procedure for 'Fulfil a new user from a local fulfilment pool'

Allocating an RSA SecurID token or Passcode OnDemand device to a user that has previously had a token and registered

If you have a user who has previously been allocated a token, for example if you have a pool of tokens that you wish to allocate as and when they need to work remotely, but when they return they give the token back.

If you leave the user on the IMC, then when you need to re-issue a token to the person, they will not need to re-register – you can allocate a new token to them, which will then issue a new PIN to them. They then simply need to register themselves a new PIN, but all other registration information will be maintained, making their life easier.

A person in this state will show on the IMC as 'Registered, no login'. If you search for the user on the IMC, from the 'Quick Links' drop-down list at the bottom of the user details, you will then be able to 'Add Authentication Device'. You will then be able to perform a standard New User Request, but the address details will be pre-filled in.

Performing Actions on Existing Users

Revoking a user

Admin Level Required: *HR Admin*

- If you wish to de-activate a user and they will not be keeping the token, then you should revoke the token. This will then allow you to re-allocate the token in future. To perform this process, follow these steps:
 - a. Go to My IMC and go to **Advanced Admin**
 - b. Go to **People** and search for the appropriate person
 - c. Choose the correct person, and then scroll down to their Authentication devices, and click on Change.
 - d. You will then see the token(s) allocated to them, and their status. Normally a user will only have one token. Click on the **Revoke** button next to the token that you would like to revoke.
 - e. If the user has given the token back to you, choose the option 'I want to be able to reallocate this token to another user'. Alternatively, if they have not given it back to you yet, choose 'I want to disable this token until I obtain it from the user'
 - f. Choose one of your local pools.
 - g. Click Revoke token now
 - h. If you indicated that you have the token yourself, then the process is finished, and this token will be available for when you do future fulfilment. If you indicated that you do not yet have the token back, then when you do obtain the token from the user, go back to the user's details page, go to **Change** on the Authentication Devices row, and then on the appropriate token row, choose **Obtained**. This token will then be available when you need to perform any local fulfilment.

From the point when you have marked the token revoked, whether or not you have indicated that the user has given the token back to you, the user will no longer be able to use that token.

If the user has more than one token, you should revoke each token in turn.

If the user is not leaving and you may wish to reallocate a token to the user in future, it is recommended that you leave the user on the IMC. In this way, you can quickly and easily reallocate a token to them in future, and the user will not need to re-register. (See *Allocating a token to a user that has previously had a token and registered*)

Alternatively, once the user has no tokens remaining (and you have marked them all as having been received by you), you can delete the user. When viewing the user's details in the IMC, choose the 'Delete User' from the Quick Links drop-down list.

Activating a user on an Authentication Node

Admin Level Required: *HR Admin or Tech Admin*

If you have an Authentication Node, and you wish to activate a user on that Auth Node, and that user already has a Signify Account and token, then you can quickly and easily enable that user on that Auth Node. You can do this in one of 2 ways:

1. From the Person View – adding a user to 1 or more Auth Nodes
 - a. In My IMC go to **Advanced Admin**
 - b. Choose the **People** menu, and then search for the user.
 - c. Select the appropriate user
 - d. Go down to Activations, and choose **Change**
 - e. Tick the appropriate Auth Node(s) that you want to add the user to, and enter the username that the user will use
 - f. Click on Save
2. From the Auth Node view – adding 1 or more users to an Auth Node
 - a. In My IMC go to **Advanced Admin**
 - b. Choose the **Auth Nodes** menu, then just press **Go** in the search area (You can enter a name or IP address if you know what you are looking for)
 - c. Choose the appropriate Auth Node
 - d. On that Auth Node's details, go down to User Activations, and choose **Change** and then tick each user that you wish to add to that Auth Node, and enter the username for that user in the appropriate field.
 - e. Then click Save

In each case, the user should be enabled on that Auth Node within the Signify system within around 10 seconds.

Depending upon your Auth Node, you may also need to add the user's details to some systems on that Auth Node – you should check with the Auth Node administrator if you are unsure.

Removing access to an Authentication Node for a user

Admin Level Required: *HR Admin*

If you wish to remove a user's access from an Auth Node, you can do this in one of 2 ways:

- From the Person View – removing a user from 1 or more Auth Nodes
 - a. In My IMC go to **Advanced Admin**
 - b. Choose the **People** menu, and then search for the user.
 - c. Select the appropriate user
 - d. Go down to Activations, and choose **Change**
 - e. Untick the appropriate Auth Node(s) that you want to remove the user's access from
 - f. Click on Save
- From the Auth Node view – removing 1 or more users from an Auth Node
 - a. In My IMC go to **Advanced Admin**
 - b. Choose the **Auth Nodes** menu, then just press **Go** in the search area (You can enter a name or IP address if you know what you are looking for)
 - c. Choose the appropriate Auth Node
 - d. On that Auth Node's details, go down to User Activations, and choose **Change** and then un-tick each user that you wish to remove from that auth node.
 - e. Then click Save

In each case, the user should be disabled from that Auth Node within the Signify system within around 10 seconds.

The user will then be unable to make any new connections to that Auth Node using SecurID. You can then, if you wish, remove any settings or data on that Auth Node relating to them.

Changing the username of a user for an Auth Node

Admin Level Required: *HR Admin or Tech Admin*

Changing the username of a user on a particular Auth Node is very straightforward. From My IMC go to Advanced Admin | People and find the person, and view the person.

Go down to the Activations row, click on *Change*. You will then get a list of all the Auth Nodes in your scope, and the ones that the selected user can access will be ticked. The username that the user will use on that Auth Node will be indicated in the appropriate field on the same row, and to change the username, simply edit it on each Auth Node that you wish to change, and then click on the *Save* button at the bottom of the page.

Authentication Nodes

Set up a new Authentication Node

Admin Level Required: *Tech Admin*

When an organisation sets up a new Authentication Node (Auth Node), the Signify service needs to be notified in order that the Authentication Servers can receive and respond to authentication requests, and so that users can be enabled on that Auth Node.

The authentication node should be set up, and connected to the Internet in its correct configuration, ready for being enabled as a Signify Auth node.

Prior to installing the RSA ACE/Agent software, or configuring the RADIUS/SecurID service, a Tech Admin should go to the My IMC area, and then to the **Add New Auth Node** link.

You can add an Auth Node for any organisation for which you are a Tech Admin. Choose the appropriate organisation, and then click 'Enter Auth Node Details'.

You are then prompted for the appropriate information for the Auth Node to be set up:

- Name – set a descriptive name that will mean something to you
- Primary IP Address is the IP Address that Signify's servers will see your traffic coming from.
 - If no address translation is being done, this should be the IP address of the machine
 - if your authnode is being hidden behind a Firewall, read the appropriate help to decide which IP address to put in here
- Choose the appropriate authentication protocol
- You can then optionally enter additional information such as Operating System and Hardware chassis, and technical notes – whilst not necessary, these can help Signify helpdesk in diagnosing a problem in future
- Login Instructions – use this area to inform your users how to connect to your authentication node. If you fill in instructions here, then on the user's list of Auth Nodes in their My IMC area, they will have a link to these instructions in case they cannot remember how to log in. This can reduce calls to your support line.
- Finally, if you already have 1 or more Auth Nodes set up, and you want to copy the set of users (along with their usernames) that are enable on that Auth Node onto this new one, then select which Auth Node you wish to copy the user list from. If you do not choose an Auth Node to copy from, then the Auth Node will be set up with no users activated on it.

You should then submit the request.

Once the Signify systems have been modified to allow the Auth Node access, you will then be notified. You can then return to the My IMC area, and choose the link to **My Auth Nodes**. You will then be able to obtain the RADIUS shared secret, or sdconf.rec file as appropriate for that Auth Node.

You obtain these details in this way because the access to it is strongly authenticated, and when you download the details this is done over a 128 bit SSL-encrypted session.

Once you have the RADIUS shared secret or sdconf.rec file, you can then continue as per the instructions for setting up that type of Auth Node.

Changing the IP address of an Authentication Node

Sometimes it is necessary to change the IP address of your Authentication node. This may be because you are moving the machine, or changing your ISP.

In this case, the best method to effect a smooth transition is described below. This allows you to get the Signify service set up in advance of the migration, such that your migration can be done whenever you wish, and also allows you a backout plan to roll back to the original working system.

You should follow the following process:

- For each Auth Node that will be moving to a new IP address, request a new Auth Node on the IMC using the IP address that it will be moving to. When you do this, there's an option to copy activations from an existing Auth Node so you can copy all the user's activations on the current live Auth Node. We suggest naming the new Auth Node the same as the existing one, but adding the word 'New' or the new ISP name in the case of an IP changeover at the end so you know which is the new and which is the old.
- If the Auth Node is a RADIUS auth node, you should also send an e-mail to customerservices@signify.net mentioning that the new auth node that you have set up is a copy, and indicate what it is a copy of. We will then ensure that the RADIUS shared secret on the new one is the same as the old one to ensure a smooth migration.
- Once you've done that for each Auth Node, Signify will process them, which will open up our firewalls, migrate the RADIUS shared secret etc. This is only done in UK working hours, so if you are doing a migration at a weekend, you are advised to do this a few days in advance so that it is all ready in advance of your migration.
- Then on the day when you're ready to move the machines to the new network addresses:
 - For Auth Nodes that are running the ACE/Agent:
 - you'll need first to backup the Node Secret in case you need to abort the ISP switchover and move back. This is stored in the registry. You should take a copy of the string in the following key, and store it in a text file. The key you should back up is: HKEY_LOCAL_MACHINE\SOFTWARE\SDTI\ACECLIENT\NodeSecret
 - Once you've moved the machines to the new IP addresses, you'll need to clear the existing Node Secret before attempting an authentication. This can be done from the ACE/Agent control panel applet, there's a button in the advanced tab.
 - For Auth Nodes that are using RADIUS to authenticate:

- You should just need to change to the new IP address because we'll have set the RADIUS shared secret to be the same on the old and the new auth nodes.

If you do need to revert back, RADIUS auth nodes will not present a problem, and you can simply switch their IP address back.

ACE/Agent auth nodes will need their Node Secret reverting back to the original one. This is best achieved by creating the above key, and copying the string back in there with the value that you stored in the text file.

Finally, once you're happy everything's stable with the changeover, the original Auth Nodes can be deleted from the IMC and the new ones can be renamed if necessary, but it may be best to wait a week or two before doing this.

Security Officer Tasks

The security officer performs two crucial tasks – setting who has each administrative role, and setting the Security Policy for the organisation.

Changing each of these is detailed below.

Allocate Administrative Roles

Admin Level Required: *Security Officer*

As described elsewhere in this document, there are a number of administrative roles that different users in an organisation may hold. Some roles may be held by multiple people, and one person can have multiple roles.

The Security Officer(s) of the company determines who may hold each role. It is recommended that there are at least two Security Officers. The Security Officer can allocate and remove admin privileges from a user.

In order to give a user an administrative role, the Security Officer should go to that user's record (for example via the My IMC | Advanced Admin | People menu)

The user's information screen, in the Staff/Admin Roles row, will show what relationships to organisations that person has. You can click on **Edit** for any of the relationships for which you are a Security Officer, and then select which Administrative roles you wish the person to have.

When setting the admin roles, some of the roles can be chosen to include only performing that type of function within your organisation, or whether you can perform that function with respect to your customers as well. You can tick each admin role that you want to apply.

Once you apply the changes, these will take effect immediately.

Set an organisation's security level

Admin Level Required: *Security Officer*

An organisation has a set of 'Security Levels' which define its security policy with regard to the Identity Management of its users. Not all organisations have the same security requirements, e.g. what for one company is an ideal, very secure policy, may for another company be too restrictive, and too difficult for users. Signify can help you set the correct security level for your requirements.

However the Security Officer(s) can change the organisation's security level as and when they see fit. The security officer can choose one of three standard settings, and can then subsequently (if they wish) fine tune the particular settings for each area.

In order to change your organisation's security level, go to your organisation's page (e.g. from My IMC | Advanced Admin | Organisations), and at the bottom, press the button 'Edit Security Levels'.

The Security levels will then be displayed on the right-hand side. You can then review the specific settings at will, and change them, or you can choose a standard set from the list box at the top.

The security levels page is broken down into a number of sections:

- 1) **General Organisation Options** – this defines what credentials your users are allowed to be allocated. This setting will automatically control the choices available to your HR Admins when requesting users
- 2) **User Security Questions** – this section sets the policy that will be applied to the number of security questions that your users must set when registering, and how many will be asked for, and the pass mark required when accessing the web helpdesk. These are automatically applied by the helpdesk when a user requests an action that requires authentication.
- 3) **Token Replacement Options** – this section defines what methods may be used to identify a user when they need to access the helpdesk. You can allow the user to be asked security questions, confirm access to an e-mail address or a mobile phone, or confirm with a notary (a trusted person that you set up as a Notary). You can then specify how many of the above methods must be successfully passed before the user can be sent a replacement token (the more confirmations are required, the higher security, but harder for your users to use). Finally you can set how the replacement should be sent to the user.
- 4) **PIN replacement options** – similar settings to token replacement, but can be configured differently in case you want different levels of protection.
- 5) **Emergency Access** - When a user loses or breaks their token, then traditionally with SecurID the user cannot gain remote access to their systems until they receive a replacement token. Signify has implemented 'Emergency Access' as a completely automated add-on to the web-based helpdesk. If your organisation has emergency access enabled, then after registering their token as broken or lost, the user will be asked if they want to enable emergency access. If they say yes, then they can generate a set of 'one-time passcodes' which can for example be sent to them by e-mail, or they can print directly from the screen (you can set how they receive them, and if any extra security steps are required before giving them emergency access). When the user wants to log in, they then simply use each number in turn from the list generated each time they log in. By enabling Emergency Access, you can set how the person is authenticated (because this actually gives access, you may wish to require more methods to confirm the identity than for a PIN replacement), and you can specify how the emergency access is made available to the end user.

Once you have made the settings you wish, you should click on Save to save your changes.

Obtaining Logs and Alerts

View Logs

You can obtain a large amount of information about your Signify service from the log interface. What you can access will depend upon your Admin Role – you will only be able to see information appropriate to your admin role. This may include:

- For HR Admins – number of users, who the users are, and their usage of the Signify service
- For Tech Admins – authentication history for your authentication nodes

- For Billing Admins – number of users, number of new users in a given period, and number of authentications

Go to My IMC | Advanced Admin | Logs and you will be presented with the appropriate search functions for your role.

Reports are by default in HTML format, in an easily viewable form in your web browser, however many of the reports can also be selected to be in CSV format so that you can load them into a spreadsheet such as Excel for further analysis.

View fulfilment status

Admin Level Required: *HR Admin or Fulfilment Operator*

If you are an HR Admin or a Fulfilment Operator, you may wish to check the status of each of the users within your scope. You can do this whether you are performing the fulfilment locally, or if Signify is performing the fulfilment for you. Simply go to **My IMC | User Fulfilment** and the various users that have not yet registered their token will be listed.

The key stages that users may be in are:

- New Requests – Not Processed. These are newly requested users that neither Signify nor a local operator has processed. If you are a local fulfilment operator and the user is due to be fulfilled by you, then you will have a 'fulfil' button next to these users so that you can allocate a token to the user.
- Users in fulfilment – Not shipped. These are users that Signify has been requested to send to the user. These users are in the process of being packed in preparation for shipping, but have not yet been sent.
- Users Ready for Activation – Not registered. These are users where the pack has been sent out, but they have not yet registered their token. In the case where the pack was sent to the user, and the PIN automatically e-mailed, this page will detail when the e-mail was sent. In the case where the requestor requested that the tokens be sent to a person (who must be an HR Administrator) who was then going to distribute the packs at a later date, then the E-mail Status column will have a button where the HR administrator can release the PIN. When they click this button, the PIN will be immediately sent to the user's e-mail address. The view will then be updated to indicate when the PIN was sent.

Other Tasks

Receiving a batch of token packs and rolling them out to users

When users are requested, an organisation can request that rather than sending tokens directly to the end user, they should be shipped via an HR Admin person. This may be so that the end user can be trained, or it may be so that the HR Admin can gradually role out the users over a period of time, as and when they require.

In this case, the token packs are all packed and addressed to the correct individuals, and sent to the HR Administrator by Signify. However the Welcome E-mails are not sent to the end user.

When the HR Administrator wishes to roll out a token to a user, before they give the pack to the user, they should go to **My IMC**, go to **User Fulfilment** and in the list of 'Users ready for activation – not registered', the HR admin will find the appropriate user, and click the '**Send E-mail**' button, which will release the Welcome E-mail.

The HR Administrator can then give the token to the user, and (depending upon the performance of the company's e-mail system) the user's Welcome E-mail should appear in their Inbox very soon, ready to register.

Managing Organisations – sub-organisations and customers

Admin level required: *Security Officer*

If you would like to manage your organisation as a number of sub-organisations, or if you wish to have users allocated that are members of staff at a customer organisation, that you would like the customer to manage, you can split administrative roles to specific groups of users and authentication nodes.

For example, if you have several offices, you may wish to allocate administrators in each office who can administer staff in that office, but not in other offices. You may wish to have a local token pool in each office for those administrators, and possibly even to have different security policies in each office.

The IMC allows you to model your organisation as a number of sub-organisations. You can then allocate the appropriate administrators and security policy to each organisation.

To create a new organisation, go to Advanced Admin, and then go to 'Organisations'. Under 'Add New Organisation' enter the name of the new organisation. Then click Go. You can then enter the name, address and postal details of the organisation. The web site is used to form the default e-mail address for users at that organisation to make the HR Admin's job easier, so if the user's e-mail address is jdoe@uk.signify.net then set the web site address to be www.uk.signify.net

Finally you can indicate the relationship between this new organisation and one of your existing organisations – so you can set them as a sub-organisation, or as a customer. You can have more than multiple levels of organisation, mapping a complex organisational infrastructure, including customers if you wish.

Glossary

User – Contact

A person on the IMC who has information stored about them but has no authentication credentials and has not registered

User – Registered

A person on the IMC who has information stored about and has registered. This registration information will then be maintained irrespective of whether they have credentials assigned to them.

Password

A credential based of the form 'something you know', that is re-useable. For example, used on it's own, the user uses the same password each time they wish to log in.

Token

A device, such as SecurID or a Smartcard, that the user carries in order to identify themselves.

SecurID

SecurID is an authentication technology developed and manufactured by RSA Security. A SecurID token displays a 6 digit number, and every 60 seconds, displays a new number. These tokens typically come as keyfob devices to attach to your keyring, but can also come in a number of other form factors, and as software that can run on a PDA or selected mobile phones. SecurID does not need any special hardware on the user's workstation.

One-Time Passcode (OTP)

A One-Time Passcode is a special type of password that can only be used once. Once it has been used, a new OTP needs to be used. Therefore it is much more secure than a re-useable (standard) password. However a method of distributing the current One-Time Passcode is required. Signify achieves this distribution using either e-mail or SMS, and the service as a whole is called Passcode OnDemand.

SMS Device

An SMS device is a mobile phone that can be used for authentication, and in order achieve authentication, a One-Time Passcode will be sent to the device.

Organisation

An organisation that has contracted with Signify to deliver authentication services to its users.

Authentication Node

The server that users log in to and which is being secured by Signify's authentication service is known within the Signify architecture as an Authentication Node (Auth Node). This may be a Firewall, a web server, a router or many other similar devices. This server is the machine either containing the data/services that the organisation is

protecting (e.g. a web server), or is the device protecting access such as a dial-in router or a firewall.

Activation

When a user is specified as being able to log into an Auth Node, they are said to be *activated* on the Auth Node. The activation has a username related to it, and if necessary a user can have a different username for each of their activations.

Agent Host

If you are used to using an RSA SecurID ACE/Server, they use the term Agent Host for the machine that users log in to. In the Signify architecture, this is known as an Auth Node.

Smartcard

Smartcards are an authentication technology that is being developed by a number of manufacturers. Smartcards can have a range of different features from simple loyalty cards, through to *crypto*-smartcards that have PKI functionality on them. Only crypto-smartcards are appropriate for authentication. Smartcards typically require a reader on the user's workstation.

Public Key Infrastructure

See PKI

PKI

A Public Key Infrastructure (PKI) is a generic term for an infrastructure based upon Public Key Cryptography, which can facilitate digital signatures, encryption of e-mail, and authentication. Public Key cryptography was invented in the 1970s, with the ingenious concept that you can use one *key* to encrypt a piece of data, but a different key to decrypt the data. One key is known as your Public Key, and can be given freely to people that you will communicate with. Your Private Key must be kept secret, ideally on a crypto-smartcard type device.

Agent Software

Some types of Auth Node can simply be connected to Signify's Authentication Network by following a simple configuration procedure. Some types of Auth Node require the Tech Admin to install some software to enable the Auth Node to communicate with Signify. For SecurID, this software is known as the Agent, e.g. the SecurID Agent for Windows.