

Authentication Node Configuration Guide



Author:	Liam Crilly
Version:	2.2
Status:	Published
Date:	27-Jul-2007
Classification:	Public

Contents

Contents	2
Introduction	2
Planning and Preparation.....	2
Locate Configuration Documentation for Your Authentication Node	3
Vendor-Supplied Documentation	3
RSA Implementation Guides.....	4
Planning Checklist	4
Submit Your Authentication Node Request.....	4
Configuring Your Authentication Node.....	6
RSA Authentication Agent Considerations	7
Downloading RSA Authentication Agent.....	7
IP Address Override.....	7
RADIUS Considerations	8
Timeout Settings	8
Next Tokencode Mode	8
Integrating web-based authentication nodes with Passcode OnDemand	8
Firewall Configuration Data	8

Introduction

Signify's Authentication Services can be integrated into your systems at any point where you need to challenge the user to validate their identity.

The devices or programs on your network that are configured to perform this challenge are referred to as your Authentication Nodes or "authnodes". Our aim is to make it as simple as possible to "Signify Enable" your chosen authnode systems to communicate with the Signify service.

This document explains how to set up your authentication node to authenticate your users using the Signify service.

Planning and Preparation

The Signify authentication service is a centralised, "on demand" managed service. Signify's authentication servers are located at two different Internet data centres in order to provide a highly-available service. This section will help you prepare to configure your authentication node. You will discover what authentication protocol to use, how to configure your authentication node to communicate with Signify.

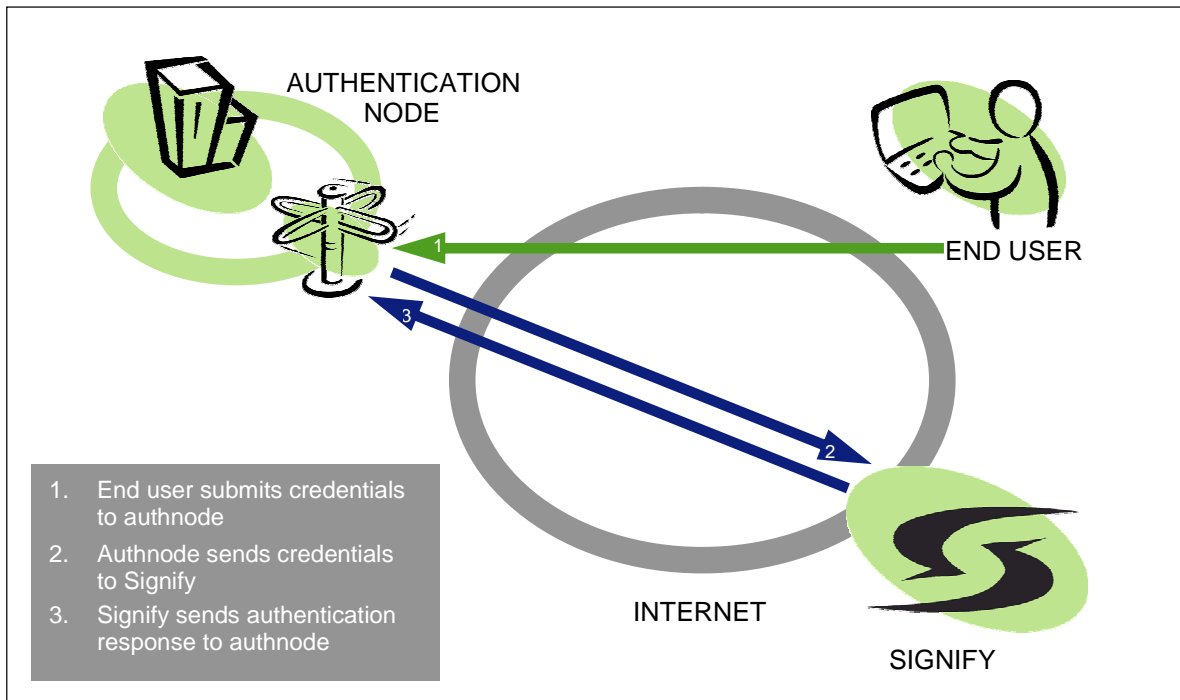


Figure 1. The sequence of events that take place during a typical authentication process.

Due to the fact that communication between your authentication node and Signify's authentication servers takes place across the Internet, there are two requirements you need to be aware of.

- 1. Authentication traffic must come from a unique, static, public IP address.**
Signify require that authentication requests come from a public, internet-routable IP address that is unique to your authentication node. If your authentication node is located on your private network (e.g. 10.x.x.x) then you will need to configure network address translation (NAT) so as to present your authentication node with an Internet address.
- 2. Your firewall must allow authentication traffic between Signify and your authnode.**
You will need to ask whoever manages your firewall to permit a specific authentication protocol between your authentication node and the Signify authentication servers. You will select an authentication protocol in the next section. For technical details of the authentication protocols and Signify's authentication servers see *Firewall Configuration Data*.

Locate Configuration Documentation for Your Authentication Node

Vendor-Supplied Documentation

Your authentication node should include information on how to configure your system to authenticate to an external server. To locate this information within the supplied documentation, search for one of the following terms:

- RADIUS
- SecurID
- SecureID
- RSA Secur

If you find information on configuring RADIUS authentication then you will use the **RADIUS (full) protocol**. If you find information on RSA SecurID authentication that you will use the **SecurID protocol**. If you find information on both protocols then RADIUS is our preferred option as it is an open standard and allows for interoperability with future authentication devices.

Make a note of which authentication protocol you have selected in the form below. Also bookmark the relevant section in your documentation for future reference. You will come back to this when the time comes to [configure your authentication node](#).

RSA Implementation Guides

As well as any documentation that may have been supplied with your authentication node, RSA maintain a library of implementation guides as part of their *RSA Secured* certification programme at www.rsasecured.com. The RSA Secured website contains documentation for many products and is a very useful resource. Signify support the vast majority of products which have an “RSA SecurID Authentication” implementation guide.

At the beginning of the implementation guide, in the Solution Summary section, check which authentication methods are supported. If “Native RSA SecurID” then you will use the **SecurID protocol**. If “RADIUS” then you will use the **RADIUS protocol**. If both are supported then RADIUS is our preferred option as it is an open standard and allows for interoperability with future authentication devices.

When reading RSA’s implementation guides, please ignore any of the following sections:

- Agent Host Configuration
- 5. RSA ACE/Server configuration

These sections relate to functionality provided as part of the Signify managed service which you will configure by using Signify’s management portal, the IMC.

At the end of the implementation guide there is a certification checklist. If you have selected the RADIUS protocol then check whether Next Tokencode Mode is supported. If supported then you will use the **RADIUS (full) protocol**, otherwise you will use the **RADIUS (without NTM) protocol**. For an explanation of next tokencode mode see *RADIUS Considerations - Next Tokencode Mode* below.

Planning Checklist

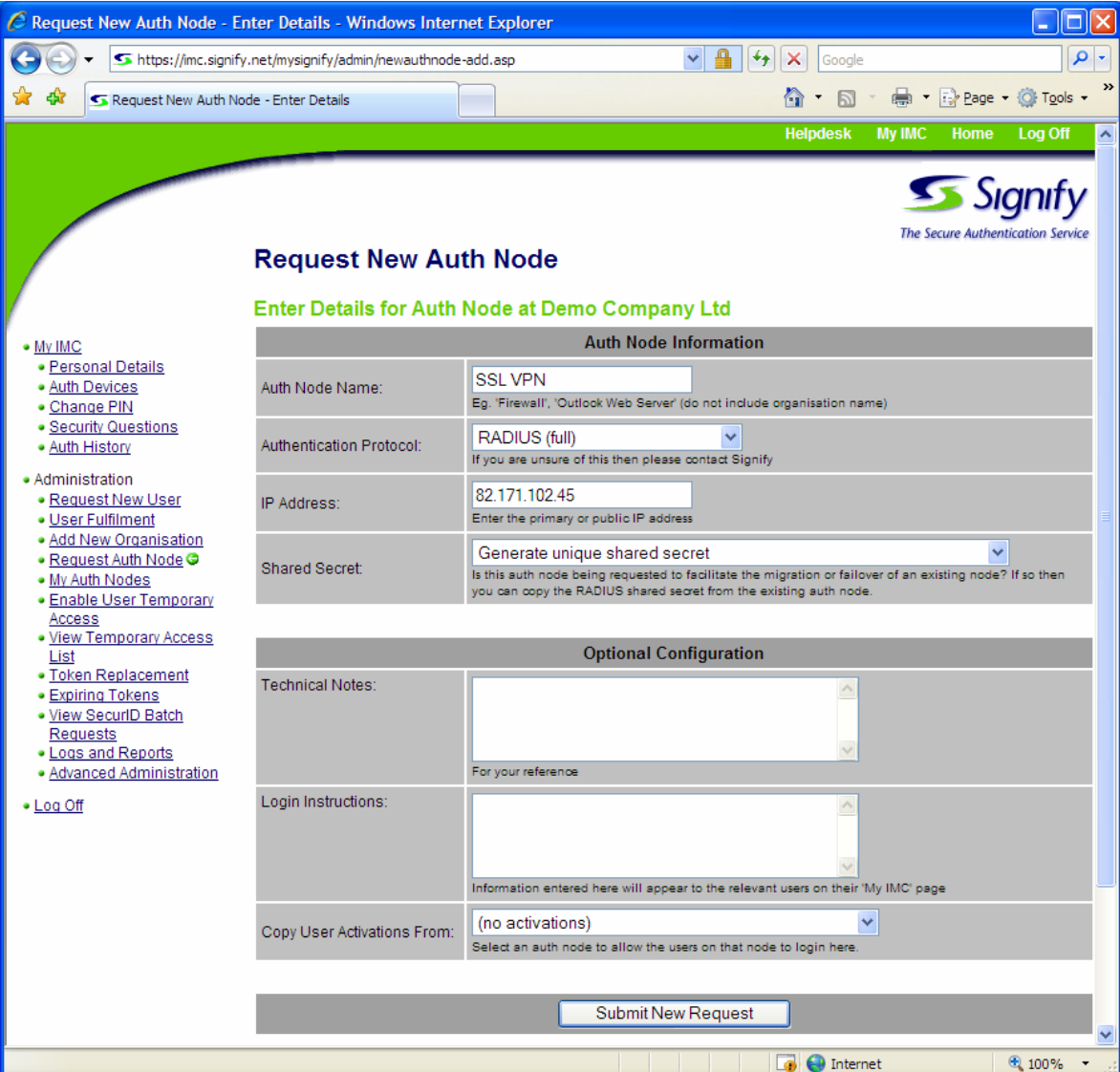
Public IP address:	
Authentication protocol:	<input type="checkbox"/> RADIUS (full) <input type="checkbox"/> RADIUS (without NTM) <input type="checkbox"/> SecurID

Submit Your Authentication Node Request

Before you can configure or test your authentication node you first need to tell Signify about it. This is done by using Signify’s Identity Management Centre (IMC) administration website (figure 2). You will need to have been assigned the “Tech Admin” role on the IMC in order to make this request. Follow these steps to create your authentication node request.

1. Login to the IMC at www.signify.net
2. From the “My IMC” page, locate the set of links on the left hand side and click on “Request Auth Node”
3. Confirm which organisation you are requesting an authnode for

4. Enter the details of your authentication node
 - Auth Node Name – the name by which your users will know this authnode. You do not need to include the organisation name, this will be automatically prefixed when viewing the authnode.
 - Authentication Protocol – choose the appropriate authentication protocol as suggested by the documentation for your authentication node.
 - For SecurID choose the appropriate ACE/Agent version for your solution.
 - For details on the difference between “RADIUS (full)” and “RADIUS (without NTM)” see *RADIUS Considerations* below.
 - IP Address – the unique, public IP address of your authentication node.
 - Shared Secret (RADIUS only) – for a new system choose to generate a new shared secret.
 - Portal URL (optional, web agent only) – the website address of the authnode
 - Technical Notes – a reference for yourself.
 - Login Instructions – some help for your users that will be displayed on MyIMC and temporary user access emails.
 - Copy User Activations From – if you already have another authnode then you can make this one available to the same users if that is appropriate.



Request New Auth Node - Enter Details - Windows Internet Explorer

https://imc.signify.net/mysignify/admin/newauthnode-add.asp

Request New Auth Node - Enter Details

Helpdesk My IMC Home Log Off

Request New Auth Node

Enter Details for Auth Node at Demo Company Ltd

Auth Node Information

Auth Node Name: SSL VPN
Eg. "Firewall", "Outlook Web Server" (do not include organisation name)

Authentication Protocol: RADIUS (full)
If you are unsure of this then please contact Signify

IP Address: 82.171.102.45
Enter the primary or public IP address

Shared Secret: Generate unique shared secret
Is this auth node being requested to facilitate the migration or failover of an existing node? If so then you can copy the RADIUS shared secret from the existing auth node.

Optional Configuration

Technical Notes:
For your reference

Login Instructions:
Information entered here will appear to the relevant users on their 'My IMC' page

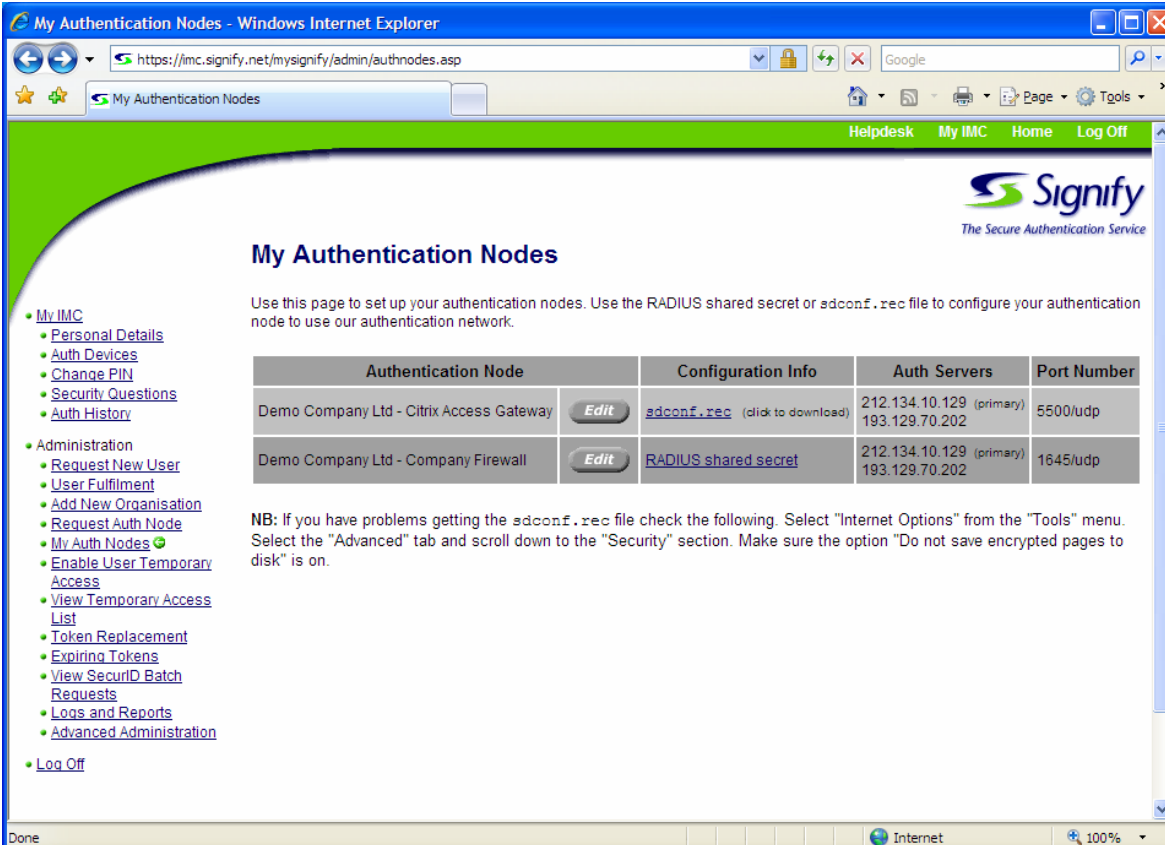
Copy User Activations From: (no activations)
Select an auth node to allow the users on that node to login here.

Submit New Request

Figure 2. Using the Signify IMC to submit an authentication node request.

Signify will typically respond to your new authentication node request within one hour (during UK business hours) and configure the Signify firewalls to accept authentication traffic from the IP address specified. When this has been completed you will receive a confirmation email to let you know that your authentication node is ready for testing.

You can now login to “My IMC” and open the “My Authentication Nodes” page which will list all of your authentication nodes along with the information you need to configure them (figure 3). This also includes the port number information required to configure your firewall to allow authentication traffic to/from Signify.



My Authentication Nodes

Use this page to set up your authentication nodes. Use the RADIUS shared secret or `sdconf.rec` file to configure your authentication node to use our authentication network.

Authentication Node	Configuration Info	Auth Servers	Port Number
Demo Company Ltd - Citrix Access Gateway	sdconf.rec (click to download)	212.134.10.129 (primary) 193.129.70.202	5500/udp
Demo Company Ltd - Company Firewall	RADIUS shared secret	212.134.10.129 (primary) 193.129.70.202	1645/udp

NB: If you have problems getting the `sdconf.rec` file check the following. Select "Internet Options" from the "Tools" menu. Select the "Advanced" tab and scroll down to the "Security" section. Make sure the option "Do not save encrypted pages to disk" is on.

Figure 3. The “My Authentication Nodes Page” with configuration information.

Normally when you request a new authentication node you will not have activated any users on it. The first user you should activate is yourself so that you can perform the initial testing. Instructions on how to do this will be sent in the confirmation email.

1. Login to My IMC at www.signify.net
2. Click on the “My Auth Nodes” link on the left hand menu bar
3. Locate your authentication node and click the “Edit” button
4. On the user activations line click the “Add” button
5. Choose your user account and enter the username you wish to use for the authnode

Configuring Your Authentication Node

Now refer to your authentication node documentation on configuring authentication. If you are using an RSA SecurID implementation guide then skip the section titled “Agent Host Configuration” – you have already completed this process by using the Signify IMC to request the new authnode.

RSA Authentication Agent Considerations

Downloading RSA Authentication Agent

If you are following an RSA SecurID implementation guide then you may be required to install the RSA Authentication Agent. Several versions are available to download from the downloads page on the Signify website.

www.signify.net/downloads

Should you be unsure of which agent to download then please contact Signify admin support for advice.

IP Address Override

If you have installed RSA Authentication Agent and your authentication node's internal IP address is different to the IP address you submitted to Signify then you will need to set an "IP address override".

The IP address is used as part of the encryption of authentication traffic between your authentication node and Signify's authentication servers. Therefore, if your authentication node is on a private/internal IP address then you must set the IP address override to be the same as the unique, public IP address that you entered when requesting the authentication node on the IMC. Follow these steps to configure the IP address override.

1. Click on Start -> Control Panel
2. Open the "RSA Authentication Agent" control panel item
3. Click on the "Advanced" tab
4. Type in the unique, public IP address for your authentication node

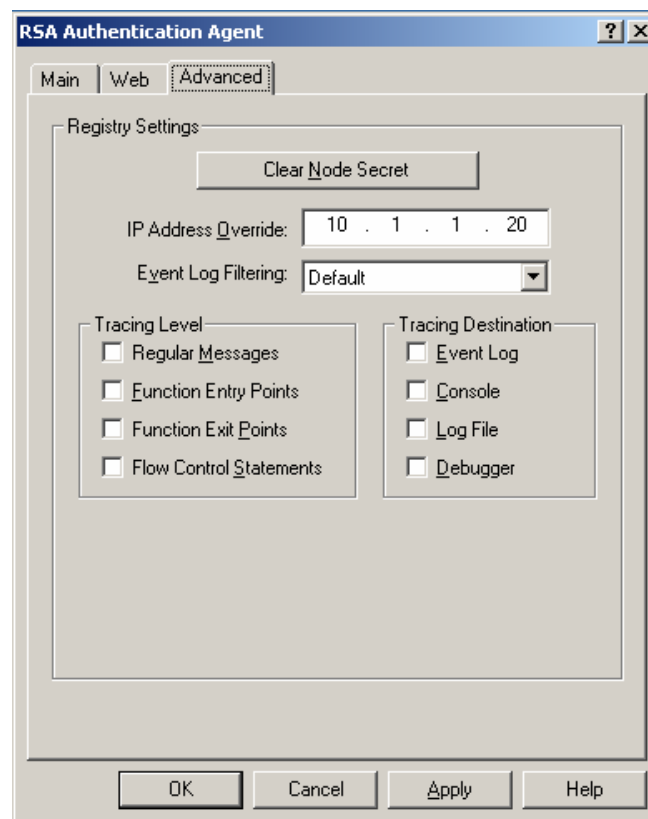


Figure 4. Setting the IP address override for RSA Authentication Agent.

RADIUS Considerations

Timeout Settings

In order to get the most benefit from Signify's highly-available authentication network, careful consideration should be given to the timeout and retry values configured on your authentication node. When authenticating with one time passcodes, it is imperative that we do not submit the same passcode twice. So if there is a problem sending an authentication request to the primary authentication server then we should not re-send to the same server and instead try the secondary authentication server.

Signify's recommended RADIUS configuration values are for a timeout of 6 seconds and no retries to the same authentication server. That is, after 6 seconds without a response the authentication node should send the authentication request to the secondary authentication server.

Sometimes you will need to work within a timeout interval imposed on you by client software or an intermediate RADIUS server. If your solution involves the users entering their login credentials to a piece of locally installed software or if your authentication node is a RADIUS server then please contact Signify admin support for configuration advice.

Next Tokencode Mode

The other area of RADIUS authentication you should consider is your authentication node's support for Next Tokencode Mode (NTM). NTM is a feature of SecurID which provides enhanced security and automatic token synchronisation. When a user is in NTM then when they login, they are prompted to enter the next tokencode displaying on their token, thereby providing two consecutive tokencodes.

Not all authentication nodes support this second login step, for example a dial-up networking or Wi-Fi solution. If you have an RSA SecurID implementation guide for your authentication node then it will include a table of supported functionality, including NTM. If your authentication node does not support NTM then you should edit the authentication protocol on the IMC to select "RADIUS (without NTM)". If you are unsure whether your authentication node supports NTM then please contact Signify admin support for assistance.

Integrating web-based authentication nodes with Passcode OnDemand

If your authentication node has a web interface and you are using Signify's *Passcode OnDemand* service then you can modify the login page to help your users request a passcode from Signify when they need to login. Please contact Signify admin support if you would like more information on how to customise the login page.

Firewall Configuration Data

Your firewall must allow the appropriate authentication protocol to the Signify authentication servers. The specific protocols and IP addresses will be discovered as you progress through this document, however the tables below show all the possible information which may be useful in getting your firewall configured quickly. This may be especially helpful if you need to make change control requests to your firewall administrators.

Your firewall will also need to allow replies to the outbound traffic, although this is typically the default configuration and will not require any special configuration.

We recommend that you allow “ping” requests so that you can check communications in the event of authentication problems.

Authentication Traffic	
RADIUS protocol	1645/UDP
SecurID protocol	5500/UDP
SecurID Windows Password Integration	5580/TCP
Ping	echo-request/ICMP

Signify Authentication Servers	
Primary 1	212.134.10.129
Primary 2	212.134.10.130
Secondary 1	193.129.70.202
Secondary 2	193.129.70.203