

Signify helps organisations to secure their computer networks. We provide a secure alternative to passwords that safely enables remote access to systems and information by delivering two-factor authentication as an on-demand hosted service.



Emergency situations, ranging from snow days to pandemics to terrorist attacks can put remote access solutions under extreme pressure. Remote access is essential in everyday business, but even more so when considered as a part of disaster recovery (DR) or business continuity management (BCM) planning. A major part of this planning is enabling staff, who don't normally do so, to work from home.

Pressure arises from not only providing extended remote access in an emergency, but also the security controls around how your network is accessed – the last thing you want to do during such incidents is add to your risk by exposing your sensitive data and information to unauthorised user access.

Signify ICE, The In Case Of Emergency Service, enables you to respond to an incident and carry on with business as usual without the need to compromise your existing security stance.

Key benefits

Reliability

- *Signify ICE* is based on Signify's 2FA service with 99.999% service availability
- Secure remote user authentication is always available, whatever and whenever it is needed

Security

- Maintain your security stance – no need to neglect 2FA in emergency situations
- Store and maintain user information and response plans in a secure, yet accessible off-site location
- Management via a secure web portal

Flexibility

- Supports existing remote workers as well as those who only require emergency access
- Users can be added manually or synchronised with your Active Directory
- Store unlimited numbers of *Signify ICE* users until you actually need them

Quick and Easy

- No physical tokens to deploy
- Compatible with all leading remote access solutions
- Automated incident management process – from user notification to one-time passcode delivery



What is Signify ICE?

Signify ICE allows the rapid deployment of two-factor authentication (2FA) to users when they need it. When an incident occurs, organisations simply login to the Signify Identity Management Centre (IMC) and select the additional users that require remote access. Signify's automated systems do the rest: Users are notified of the incident by email or SMS and are directed to a website. From there they receive further information about the incident and set a secret PIN for themselves before being directed to the organisation's remote access solution. The remote access login page allows the user to request a One Time Passcode (OTP) to be sent to their mobile phone. By entering their secret PIN and OTP, the user is securely identified with two-factor authentication.

A Complete Managed Service

The successful deployment of two-factor authentication takes more than just technology; you also need to implement a framework of policy, procedures, logistics and user support. These are automated through key features of our service:

Authentication Infrastructure: Security and reliability is designed in and implemented across multiple data centres, to deliver and validate one time passcodes every time.

The Identity Management Centre (IMC): Manage all aspects of your service through our easy-to-use web portal. A *Signify ICE* Incident Management page supports the whole incident management process including detailed incident monitoring tools, document hosting to support business continuity and defined templates for populating communication messages and landing pages.

Administrator Helpdesk Tools: Administrators have access to helpdesk tools to help them solve common problems such as user PIN resets.

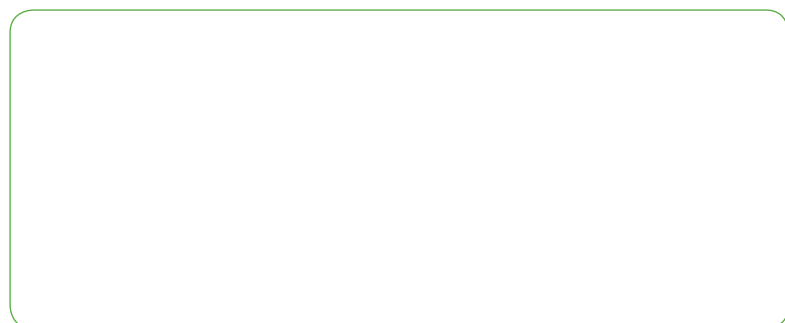
Passcode OnDemand Functionality:

Signify ICE has all the same functionality and options as Signify's full *Passcode OnDemand* service.

Included Features:

- Unlimited number of ICE users, created through a web-based interface or by synchronisation with Active Directory
- Web based incident management interface
- Secure storage for incident response plans
- End user notification system using both SMS and email
- Notification response process guides the user to your remote access solution

Authorised partner:



The Secure Authentication Service

info@signify.net **www.signify.net**

+44 (0)1223 472572