Phone:
+ 353 1 4294000

Web
www. allnone.ie

Address
48/49 Western Parkway Business Park
Lower Ballymount Road
Dublin 12
Ireland

BE and Login Security

A Managers guide to Logins and Login Security

Author: Philip Lacey
Version: 1-4
Date: 2013-10-21

Phone:
+ 353 1 4294000
Web
www. allnone.ie
Address
48/49 Western Parkway Business Park
Lower Ballymount Road
Dublin 12
Ireland

1. Overview

1.1 Introduction

For any solution, security is paramount. No solution can be 100% secure unless it is not actually plugged into the Internet or even a local network. There is therefore a continuous tension between risk and ease of use. The more secure the solution, the less user-friendly it becomes.

This document explores the most popular security options and currently available. Most of us are familiar with these solutions but we have probably never examined the issues associated with login security.

This document is intended to outline the options available from Business Express for business managers seeking to make informed decisions as to what security options would serve their organisation best.

There is a simple table at the end of the document to help you decide the options best for your organisation.

1.2 Acronyms and abbreviations

API	Application Programming Interface
ASA	Adaptive Security Agent
BE	Business Express
DDos	Distributed Denial of Service
EC2	Elastic Compute Cloud
HTTP	Hyper Text Transfer Protocol
HTTPS	Hyper Text Transfer Protocol Secure
IaaS	Infrastructure as a Service
IP	Internet Protocol
ISO OSI	International Standards Organisation Open Systems Interconnectivity
IT	Information Technology
LDAP	Lightweight Directory Access Protocol
MFA	Multi-Factor Authentication
NOC	Network Operations Centre

OTC	One Time Code
PaaS	Platform as a Service
PPS	Personal Public Service
RSA	Ron Rivest, Adi Shamir and Leonard Adleman
SaaS	Software as a Service
SC	System Champion
SecC	Security Champion
SLA	Service Level Agreement
SMS	Short Messaging Service
SSO	Single Sign On
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol / Internet Protocol
TFA, T-FA, 2FA	Two Factor Authentication
UK	United Kingdom
US	United States of America
USB	Universal Serial Bus

Phone:
+ 353 1 4294000
Web
www. allnone.ie
Address
48/49 Western Parkway Business Park
Lower Ballymount Road
Dublin 12
Ireland

1.3 Version History

Version	**1-4**
Date	2014-03-31
Author	Philip Lacey
Modifications	Inclusion of the Security Options Matrix v1-0.xlsx in section 5.3

Version	**1-3**
Date	2013-10-22
Author	Chris Thomson
Modifications	Language and context revision

Version	**1-2**
Date	2013-10-22
Author	Philip Lacey
Modifications	Inclusion of the Security Matrix and Default BE Security Matrix

Version	**1-1**
Date	2013-10-21
Author	Philip Lacey
Modifications	Restructuring of options to facilitate logic flow

Version	**1-0**
Date	2013-10-21
Author	Philip Lacey
Modifications	Initial document draft

Phone:
+ 353 1 4294000
Web
www. allnone.ie
Address
48/49 Western Parkway Business Park
Lower Ballymount Road
Dublin 12
Ireland

1.4 Contents

Phone:
+ 353 1 4294000
Web
www. allnone.ie
Address
48/49 Western Parkway Business Park
Lower Ballymount Road
Dublin 12
Ireland

2. Common Terms

2.1 On-premise vs. Hosted

Most business users these days are conversant with the terms *client* and *server*. A client is your computer whilst a server is a machine that is dedicated to doing work for your organisation. Servers have a number of roles including file storage, email management and database management and an on-premise solution is one where the server is under your direct control.

Today, many organisations employ third parties to manage the server function and this is usually referred to as a hosted solution. The various levels of hosting are characterised as:

- Infrastructure as a Service (IaaS) provides a secure building and facilities for your server
- Platform as a Service (PaaS) means you rent a server and someone else manages its maintenance
- Software as a Service (SaaS) means all your organisation needs is to log into the solution to use it

Some SaaS solutions require you to install custom software on your computer, pure SaaS does not.

Your security concerns will depend on the solution you require. SaaS leaves you with the least to do, but does mean you leave a lot of security decisions to your provider.

All n One's Business Express is a pure SaaS solution hosted in Dublin by Sungard. This partnership provides a range of security features and infrastructure options which means that end users don't have IaaS or PaaS considerations. Detailed technical security documentation is available from All n One on request.

Phone:
+ 353 1 4294000

Web
www. allnone.ie

Address
48/49 Western Parkway Business Park
Lower Ballymount Road
Dublin 12
Ireland

SaaS is a relatively new phenomenon and IT security staff are rightly keen that the security of the solution is at the forefront, with understandable concerns around how company data is managed. However, with planning and understanding, a useful and realistic risk assessment can be made.

In truth, hosted solutions are often more secure than on-premise solutions but there remain a number of security decisions to make and this document will guide you through the various options.

Phone:
+ 353 1 4294000
Web
www. allnone.ie
Address
48/49 Western Parkway Business Park
Lower Ballymount Road
Dublin 12
Ireland

2.2 Client Database

To All n One, the security of your data is secure is supreme. Each client has their own discreet database which hosts their data and the database is identified by the organisation's name.

2.2 System Champion

The System Champion (SC) is the primary link between your organisation and All n One. The SC is provided with up to eight hours free initial training to familiarise them with the system and teach them the basic functions. System operational queries should also be routed through this System Champion and they are copied in on system notices.

2.3 Security Champion

Larger organisations manage the security of their hosted solutions themselves and commonly nominate a Security Champion (SecC), versed in the security options of BE and aware of security considerations.

2.4 Username

A username is a unique identifier and can take many forms but most of us use our own name. More recently an email address or mobile phone is used.

By default Business Express uses *Firstname* / *Surname*, however you can use a number of fields for the unique identifier.

- Username (Firstname Surname combination)
- Work Email address
- PPS number
- Unique Field (this allows a custom identifier to be used)

2.5 Password

A password is a secondary identifier that should be known only the user. In BE a user's password is initially selected by the person setting up the user and then changed at first user login.

Passwords can be frustrating and complicated with different tools having widely different rules for what is or is not acceptable. Password management techniques have been developed to ease some of the pain but this still remains the primary challenge for all systems developers.

Section 4.1.2 of this document explains the password options available in BE.

2.6 Tokens and Cookies

When a client requests a web page and that page is a *secure* page, it is important that the client lets the server know that the user is valid. It would be unsafe to retransmit the username and password every time you request the page so instead, when you first login correctly, a temporary token is created against your account and stored in your cookies [temporary pieces of information stored in your browser]. Tokens are system managed and usually very complicated.

Consider the scenario

1. Client: I want to log please
2. Server: Please provide a username and password
3. Client: Here is my username and password
4. Server: Ok, I have validated that, here is your token
5. Client: Thanks, I know I must transmit my username and token for every secure page I request

So long as your browser remembers the username and token, you will be able to access the page.

Phone:
+ 353 1 4294000
Web
www. allnone.ie
Address
48/49 Western Parkway Business Park
Lower Ballymount Road
Dublin 12
Ireland

2.7 TCP/IP

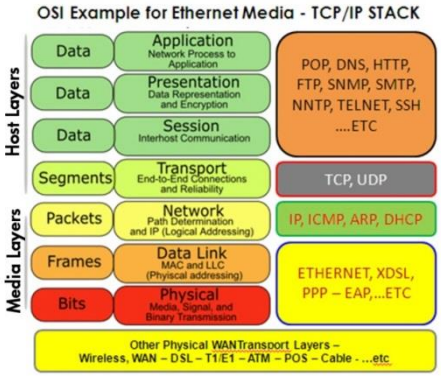
TCP/IP stands for Transmission Control Protocol / Internet Protocol and is the common term for what most of the Internet is built on.

The Internet could be considered a giant postal system. Take a message, wrap it in an envelope [packet] and pass it to another computer to deliver. There are envelopes inside envelopes, with addressing and content being more specific with each layer.

At base, the envelope you send is simple. Inside that envelope are messages for a TCP programme and the computer knows what to where, based on the IP address info in the TCP envelope. At the top of the heap is the message itself which can do further checks to ensure that delivery is accurate. This concept is vital to security.

It make take many packets to deliver one message and therefore packets have an order number and checking information so they can be reassembled in the right order. In some cases the client may resend a packet that didn't come through correctly. All of this happens in milliseconds, around the world, daily!

This process is built on the ISO OSI Model (International Standards Organisation Open Systems Interconnectivity Model) on seven layers with layers 3 and 4 being IP and TCP respectively.



From: http://blog.anuesystems.com/tag/vlan-tcpip-stack/

Phone:
+ 353 1 4294000
Web
www. allnone.ie
Address
48/49 Western Parkway Business Park
Lower Ballymount Road
Dublin 12
Ireland

2.8 Multi-Factor Authentication

Requesting a number of authentication factors for the login, including a physical barrier item.

Definition

Multi-factor authentication (aka MFA, Two-factor authentication, TFA, T-FA or 2FA) is an approach to authentication which requires the presentation of two or more of the three authentication factors: a knowledge factor (something only the user knows), a possession factor (something only the user has), and an inherence factor (something only the user is). Each factor must be validated by the other party for authentication to occur.

http://en.wikipedia.org/wiki/Multi-factor_authentication

There are a number of hardware options that manage this, from smart cards, to small keys that display One-Time-Codes (OTC).

RSA SecureID

http://www.emc.com/security/index.htm?nav=1

Feitian OTC solutions

http://www.ftsafe.com/product/otp

SafeNet SaaS solutions

http://www.safenet-inc.com/data-protection/authentication/secure-cloud-access/

Phone:
+ 353 1 4294000
Web
www. allnone.ie
Address
48/49 Western Parkway Business Park
Lower Ballymount Road
Dublin 12
Ireland

2.9 Single Sign On

Single sign-on allows you to log into one service and it creates a token for other systems to use, thus negating the requirement for the user to log into multiple systems.

Definition:

Single sign-on (SSO) controls access to multiple related, but independent, software systems. The user logs in once and gains access to all systems without being prompted to log in again at each of them. Conversely, Single sign-off terminates access to multiple systems.

http://en.wikipedia.org/wiki/Single_sign-on

An example of SSO is LDAP (Lightweight Directory Access Protocol). The user signs into their computer at the start of the day and that's the only login for the entire day. Set up of this solution requires one of two configurations. One requires the LDAP server to push a token into BE when the user logs in whilst the other gives BE access to the LDAP server to query the user's validity. Both solutions require your IT department to be involved in the setup.

There is a reduced security option within BE which is commonly used with phone systems and involves using a set token, a username and restriction by IP address. This allows screen pops to log the user into BE as and when a call arrives.

2.10 OAuth

OAuth allows a service provider to permit a user to log into another service.

For example; a company provides a service that requires users to have a Facebook account. The company facilitates the user logging into their Facebook account and if they log in properly they can use the service. The pro of this is the reduced development and security management for the company and the user (they only have one set of usernames and passwords). The con is that the user must have a Facebook account and there is a dependence on the Facebook security.

Definition:
OAuth stands for Open standard for Authorization and provides a method for clients to access server resources on behalf of a resource owner such as an end-user. It also provides a process for end-users to authorize third-party access to their server resources without sharing their credentials (typically, a username and password pair) using user-agent redirections.

2.11 Public Cloud vs. Private Cloud

A public cloud is an IaaS, PaaS and SaaS provided on shared equipment; often you have more than one paying client sharing the same equipment, e.g. the same server. This solution is specified in our terms and conditions, and is generally cheaper than putting the solution in place yourself *because* it's shared. Public clouds too, tend to have restricted security guarantees and location of the server may not be specified. A popular example of a public cloud solution is Amazon's EC2.

A private cloud provides the high availability of a cloud solution but is provided for one dedicated purpose. All n One have use a private cloud for the delivery of BE to ensure security and compliance with Irish Law. US companies mean that the US government are entitled to view the data they store regardless of the client. UK companies providing cloud solutions are the same as they are subject to the anti-terror laws as a result of 7/7.

Phone:
+ 353 1 4294000
Web
www. allnone.ie
Address
48/49 Western Parkway Business Park
Lower Ballymount Road
Dublin 12
Ireland

3. Infrastructure Security

3.1 Availability of Security Measures

A major security concern of course is the availability of the solution and its important to ensure that the service delivers the lowest possible, if not zero, downtime. BE has its own security management engine which means when the BE service is available the security engine is available.

Some clients prefer to use Multi-Factor Authentication or OAuth. It is worth considering the availability of the third parties and also the availability and management of the physical keys.

Locking a user account down to a specific IP address ensures that the facilities are only accessed from the designated point. If, however, the Internet connection should fail the service would become unavailable.

BE has been 100% available since October 2008. This is due to the high availability architecture which consists of a number of tiers including a load balancer which swaps servers automatically if another is busy.

3.2 Communications Security

As mentioned in section 2.7, TCP/IP is vital to communications security. Packets of communication between user and server pass through different devices which can capture packets and reconstruct messages. If the packets contain passwords a hacker can sit and watch for a password packet to pass through it so there are security approaches available to counter this threat.

The first option is to encrypt the contents of the envelopes so even if a hacker breaks in, the contents of the packet are encrypted. Encryption does have side effects though; the better the encryption the longer the data

becomes and the more encoding and decoding must be done by the client and by the server. For this reason there are a number of approaches available.

The most commonly accepted method for content encryption is HTTPS (Hyper Text Transfer Protocol – Secure). When browsing the net an HTTPS connection works exactly the same as an HTTP connection except that all contents are encrypted, including the user name and password.

HTTPS is not 100% secure, no solution is, but it is secure enough to be the method used by banks the world over and it's the most user friendly.

There is also a mountain of security management to ensure that malformation of packets is caught and prevented. Techniques include checksums, constant transmission of IP addresses and IP blocking.

Business Express has inbuilt routines that swap a user back if they accidentally try to move off HTTPS. Token and user account management combinations reduce the likelihood of effective hacker attack. The Sungard Network Operations Centre (NOC) performs 24 / 7 monitoring and auto adaptation to the most common communications attacks such as DDos (Distributed Denial of Service) and Brute Force hacking. In addition there is a Cisco Adaptive Security Agent (ASA) within the solution architecture.

3.3 Secure Physical Access

One of the most common types of security breaches is simply sticking a USB key into the server and downloading files from the server. All n One and Sungard to provide physically secured access to the Business Express private cloud. If you'd like further details on this or any other aspect of our security please contact us and we'll be happy to provide details.

Phone:
+ 353 1 4294000
Web
www. allnone.ie
Address
48/49 Western Parkway Business Park
Lower Ballymount Road
Dublin 12
Ireland

3.4 Social Engineering Security

A growing area of security concern is social attacks: a person ringing up, pretending to be a user, to get their password changed is one example. For this reason user account change is managed by System or Security Champions these and All n One will only make changes through these nominated people using documented and agreed procedures.

Phone:
+ 353 1 4294000
Web
www. allnone.ie
Address
48/49 Western Parkway Business Park
Lower Ballymount Road
Dublin 12
Ireland

4. User Interface Security

4.1 General login process

4.1.1 Login Security

The login screen of any system requires the provision of authentication items; user name, password and any other security tokens. In BE the user name can be applied via a drop down list or using a free text box. The drop down list makes it far easier for a user to find their account but advertises all accounts on the system. The free text box is more secure but requires the user to remember their user name.

The second option is matching the type format. Is philip.lacey@allnone.ie the same as Philip.Lacey@allnone.ie? Globally email addresses are case insensitive so it's important to consider whether the user name should be precisely the same as that listed in the account details. This is called Boolean matching and if it's turned off then Joe Bloggs and joe blogs, for example, would both be considered both acceptable. If Boolean matching is turned on, then they would be considered as the same.

4.1.2 Password Security

As above, the first consideration here is Boolean password matching.

For stronger user verification but without the need to move to Multi-Factor authentication it is possible to use a second level password. Examples of this are bank logins where details from a second level password are required. Again Boolean matching is possible and it's also possible to extract a random numbered character from the data. This is done to reduce pattern matching for users who log in frequently because different combinations of characters are used on different log ins.

4.1.3 Hardening security messages

Hardened security messages means that the user is provided with either more or less detail. For example; a user name is put into the system but is not found. The message can be *User not found* which is helpful to a valid user but it also tells someone illegitimate trying that the user name does not exist. Hardening the security messages would change the message to *User / Password combination not found*. This means that this combination of user name, password and potentially second level password were not correctly supplied.

4.1.4 Password cycling

Cycling passwords is an effective method not only of preventing access but also *removing* access if an account has been compromised but it does require the user to remember their password sequence.

The most common trigger of password cycling the password is time but there are others such as number of logins, number of failed logins or change of machine. The time window itself can also be controversial. Too short and it can annoy users, too long and it becomes an ineffective security measure. If you must recycle, 90 days is a usual base line.

Most systems allow the user to supply their own password so when a user is forced to change their login they are presented with a password change box. The first field has to be the old password to prevent casual or malicious password changes.

The password is often required to be of a sufficiently complex type. Eight characters or more ensures that the combinations are in the billions which is enough to prevent brute force hacking. Forcing the use of capital and lower case characters as well as special characters increases the number of possible combinations. The usual descriptive terms for password strength are: Weak, Medium, Strong, Best and you can set a minimum strength requirement.

Sometimes, when the system has insisted on a password change some (crafty) users go straight back in and reset their password to one they are familiar with. This would still count as a valid password change so a password history can be implemented to prevent resetting to an old one. A history of about 8 passwords is normal.

For clients whose phone system is linked to Business Express we have implemented the ability to have a secondary session key for the phone system which allows the phone system to log the user in on call arrival at the agents' desk using of Locked Session Keys.

4.1.5 Lockouts and Options

If a password is used many times in quick succession, it can indicate a brute force attack. For this reason, the system can keep a count of how many failed attempts occurred on an account. When this count reaches a pre-set limit, the account is locked.

4.1.6 Password Recovery

Strategies for releasing a locked account vary but *Release in 24 hours* or *human intervention required* are the two most common approaches. Release in 24 hours is less secure and frustrating for a user if they genuinely forget but human intervention can raise resource issues. Again social engineering attacks needs to be trained and secured against if offering password / lockout support.

Email Token

On request the password is emailed to the email address that was set up with the account. Usually the password is reset to a random password which is emailed and can be collected from the mailbox.

SMS Reminder

On request the password is texted as is to the mobile number set up with the account.

Security questions

On account setup there are a number of other questions that get filled in. These questions are then displayed to allow the user reset their account on successful answer. Usually three questions are used with the reset process choosing one at random. Matching on the answer is not Boolean.

4.1.7 System Use Security

Using the system and leaving a screen open can be a security risk, especially if the solution is being used in heavily populated areas. Auto logout allows the system to automatically logs out the user after a given time period at which point a custom message can also be displayed on screen for the user.

4.1.8 API Security

An API allows external systems to interact with a solution (in this case Business Express) without the need for human intervention. These automated login engines pose their own security risk and for this reason BE separates the User Interface, username and password and an API username and password so that external systems compromise is a minimum impact on the User Interface.

Phone:
+ 353 1 4294000
Web
www. allnone.ie
Address
48/49 Western Parkway Business Park
Lower Ballymount Road
Dublin 12
Ireland

5. Risk Vs. Ease of Use

5.1 Overview

It is now possible to choose from a wide variety of security options. Some cost more than others and have more intricate technical setups with longer lead times. The matrix below provides a list of these options.

Risk Vs. Ease of Use is generally evaluated by a security specialist but answering to the options will more clearly define your requirements for the evaluation of your security team.

Phone:
+ 353 1 4294000
Web
www. allnone.ie
Address
48/49 Western Parkway Business Park
Lower Ballymount Road
Dublin 12
Ireland

5.2 Matrix

Area	Question	Possible Answers	Selected Choice
OAuth Services			
	Is OAuth to be used?	Yes, No	
	Is an OAuth service available?	Facebook, Twitter, LinkedIn, Other	
	Do all potential users have an account with the provider?	Yes, No	
Single Sign On			
	Is Single Sign On to be used?	Yes, No	
	Is a single sign on solution available internally?	Yes, No	
	SSO Provider	LDAP, Other	
Multi-Factor Authentication			
	Is Multi-Factor Authentication to be used?	Yes, No	
	Is an independent security verification supplier available?	RSA, Feitian, SafeNet, Other	
	Have all users been supplied with the appropriate physical token generators?	Yes, No	
	Are the availability considerations enough to warrant multiple suppliers?	Yes, No	

Phone:
+ 353 1 4294000
Web
www. allnone.ie
Address
48/49 Western Parkway Business Park
Lower Ballymount Road
Dublin 12
Ireland

Login Options			
	Username Field?	Surname, First name, Email, Mobile, Account Number, Other	
	Drop Down List / Free Text?	Drop Down List / Free Text	
	Username Boolean matching?	Yes, No	
	Password Boolean matching?	Yes, No	
	Second level password usage?	Yes, No	
	Second level field?	Email, Mobile, Account Number, Other	
	Second level Boolean matching?	Yes, No	
	Second level - Random character selection?	Yes, No	
	Harden security messages?	Yes, No	
Password changing options			
	Password strength / complexity?	None, Weak, Medium, Strong, Best	
	Timed password changing?	Yes, No	
	Time window?	Number (in Days)	
	Password history?	Yes, No	
	Password history length?	Number	
	Locked session keys?	Yes, No	
Lockout options			
	Lockout accounts?	Yes, No	
	# Failed Attempts?	Number	
	Release strategy?	Timed, Human Intervention	
	Timed Release	Number (in Hours)	

Phone:
+ 353 1 4294000
Web
www. allnone.ie
Address
48/49 Western Parkway Business Park
Lower Ballymount Road
Dublin 12
Ireland

Password Recovery			
	Strategy?	Human Intervention, Email Token, Text Reminder, Security questions	
	Human Intervention - Contact method	Email, Phone	
	Human Intervention - Help SLA	Number (in hours)	
	Email Reminder - Address from	Email address	
	SMS Reminder - Number / Name from	Up to 16 numbers or Up to 11 Alphanumeric characters	
	Security Questions - Questions	Questions to ask	
System Use Security			
	Use Inactivity Logout	Yes, No	
	Inactivity Logout Time	Number (in minutes)	
	Inactivity Logout Message	Message	

Sample Excel Version

Security Options Matrix v1-0.xlsx

Phone:
+ 353 1 4294000
Web
www. allnone.ie
Address
48/49 Western Parkway Business Park
Lower Ballymount Road
Dublin 12
Ireland

5.3 Business Express Default Matrix

Area	Question	Possible Answers	Selected Choice
OAuth Services			
	Is OAuth to be used?	Yes, No	No
	Is an OAuth service available?	Facebook, Twitter, LinkedIn, Other	N/A
	Do all potential users have an account with the provider?	Yes, No	N/A
Single Sign On			
	Is Single Sign On to be used?	Yes, No	No
	Is a single sign on solution available internally?	Yes, No	N/A
	SSO Provider	LDAP, Other	N/A
Multi-Factor Authentication			
	Is Multi-Factor Authentication to be used?	Yes, No	No
	Is an independent security verification supplier available?	RSA, Feitian, SafeNet, Other	N/A
	Have all users been supplied with the appropriate physical token generators?	Yes, No	N/A
	Are the availability considerations enough to warrant multiple suppliers?	Yes, No	N/A

Phone:
+ 353 1 4294000
Web
www. allnone.ie
Address
48/49 Western Parkway Business Park
Lower Ballymount Road
Dublin 12
Ireland

Login Options			
	Username Field?	Name, First name, Email, Mobile, Account Number, Other	Name
	Drop Down List / Free Text?	Drop Down List / Free Text	Drop Down List
	Username Boolean matching?	Yes, No	No
	Password Boolean matching?	Yes, No	No
	Second level password usage?	Yes, No	No
	Second level field?	Email, Mobile, Account Number, Other	N/A
	Second level Boolean matching?	Yes, No	N/A
	Second level - Random character selection?	Yes, No	N/A
	Harden security messages?	Yes, No	No
Password changing options			
	Password strength / complexity?	None, Weak, Medium, Strong, Best	None
	Timed password changing?	Yes, No	No
	Time window?	Number (in Days)	N/A
	Password history?	Yes, No	No
	Password history length?	Number	N/A
	Locked session keys?	Yes, No	No
Lockout options			
	Lockout accounts?	Yes, No	No
	# Failed Attempts?	Number	4
	Release strategy?	Timed, Human Intervention	Human Intervention
	Timed Release	Number (in Hours)	24

Phone:
+ 353 1 4294000
Web
www. allnone.ie
Address
48/49 Western Parkway Business Park
Lower Ballymount Road
Dublin 12
Ireland

Password Recovery			
	Strategy?	Human Intervention, Email Token, Text Reminder, Security questions	Human Intervention
	Human Intervention - Contact method	Email, Phone	Phone
	Human Intervention - Help SLA	Number (in hours)	4
	Email Reminder - Address from	Email address	businessexpress@allnone.ie
	SMS Reminder - Number / Name from	Up to 16 numbers or Up to 11 Alphanumeric characters	BusExpress
	Security Questions - Questions	Questions to ask	N/A
System Use Security			
	Use Inactivity Logout	Yes, No	No
	Inactivity Logout Time	Number (in minutes)	N/A
	Inactivity Logout Message	Message	N/A