mindaclient

Data Protection and Security at MindaClient

Data Protection

The Data Protection Act 1988 and the subsequent Data Protection (Amendment) Act 2003 (which brought Ireland into line with the EU Data Protection Directive 95/46/EC) defines the Eight Rules of Data Protection to which Data Controllers must comply.

Obtain and process information fairly
Keep it only for one or more specified, explicit and lawful purposes
Use and disclose it only in ways compatible with these purposes
Keep it safe and secure
Keep it accurate, complete and up-to-date
Ensure that it is adequate, relevant and not excessive
Retain it for no longer than is necessary for the purpose or purposes
Give a copy of his/her personal data to an individual, on request

MindaClient operates in compliance with all of the above directives.

Encryption

All data going to and from MindaClient is encrypted. All communication with our servers is over HTTPS (HTTP Secure) which guarantees two-way data encryption between our clients and our servers. We use the internationally recognised 256-bit encryption standard, SHA2 256, which is considered strong encryption, and is used by governments and leading financial institutions around the world. Our servers sit behind firewalls for maximum protection.

System & Password Security

There is system level security that only allows users see what sections that the administrator has given them access to. There is a secure password required for all users to access the system. Users have the facility to change their password once they first access MindaClient, and also on an ongoing basis.

Network Infrastructure

The network has been built and deployed using state of the art Cisco Routers by our own in-house network administration team. Utilising redundant fibre based connections and multiple sites, we now have over 5Gbps of uncontended transit connections and peering links.

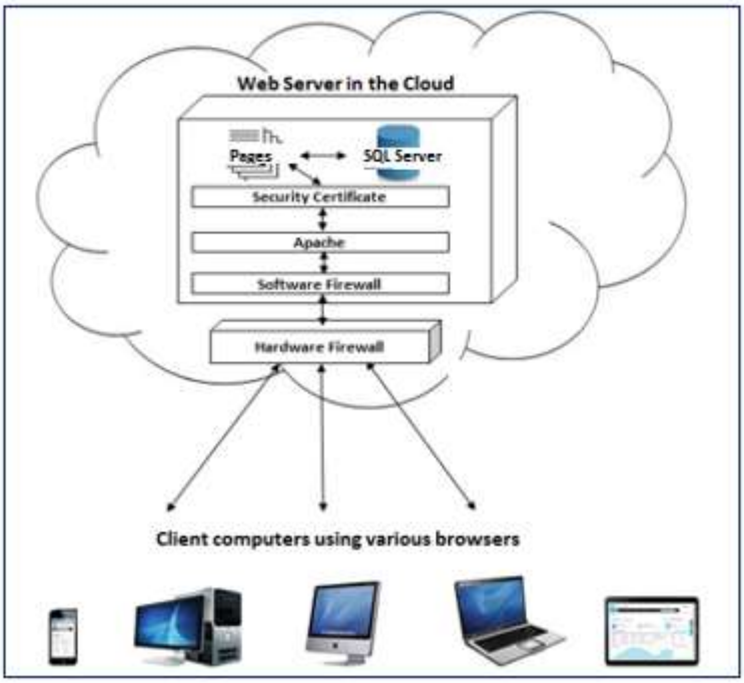


Diagram outlining the MindaClient Infrastructure

These Network facilities at the data centre we use includes:

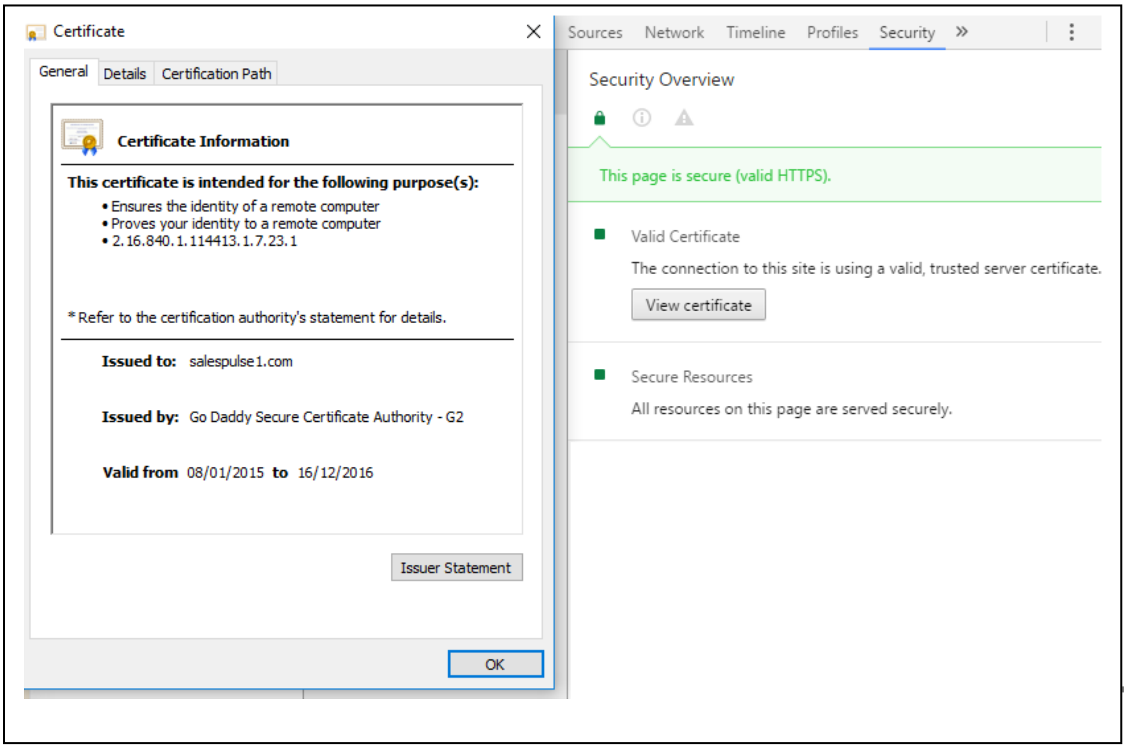
- ✓ On-site fibre optic connectivity to global transit providers
- ✓ The fastest possible connection speeds
- ✓ Multi-layered physical security
- ✓ Environmental controls
- ✓ Power resilience utilising multiple National Grid connections
- ✓ On-site generators with UPS and battery systems for power backup with transparent failover
- ✓ Fire detection and suppression
- ✓ Water leak detection
- ✓ CCTV and recording
- ✓ Site resilience for our core services, so that even in the very unlikely event of a data centre failing, our services can continue running.

Security Certificate

We have an up to date Thawte SSL certificates on all our servers, and all traffic to and from the server is carried on a secure, encrypted connection using https:// instead of http://

You will notice a small lock on the screen when you are access your system.

This indicates that you are accessing the information over a secure connection. Our servers have SSL certificates that use strong SHA-2 256 BIT encryption, which is the current industry standard.



Certificate Information

This certificate is intended for the following purpose(s):

- Ensures the identity of a remote computer
- Proves your identity to a remote computer
- 2.16.840.1.114413.1.7.23.1

* Refer to the certification authority's statement for details.

Issued to: salespulse1.com

Issued by: Go Daddy Secure Certificate Authority - G2

Valid from 08/01/2015 **to** 16/12/2016

Security Overview

This page is secure (valid HTTPS).

Valid Certificate

The connection to this site is using a valid, trusted server certificate.

Secure Resources

All resources on this page are served securely.

Automatic logout

If you leave the system idle for 60 minutes without using it you will be automatically logged out and you will have to log in again. This is intended to strengthen the confidentiality to ensure that if a user leaves the system on and leaves their desk then someone else in the office will not gain access to the system.

Password Protection

Only persons with a secure password can access the system. It is the client's responsibility to ensure that passwords are not revealed or given to people who should not be given access to the system.

Hierarchical Levels

There is a detailed hierarchy build into the system which ensures that different classes of users only see the information that they are allowed to see. These levels can include different levels of administrator access as well as ordinary users.

The full administrator would normally have control of the users rights and levels.

Backup

A nightly back up is taken of all the information on our secure server. In addition to this a weekly secure offsite backup is taken of all the data on our server(s). This ensures that information is continuously protected in the most up-to date manner.

Confidentiality

All of our staff have signed legal client confidentiality agreements.

The Eight Rules of Data Protection as quoted on the Data Commissioners website www.dataprotection.ie

You must :

- Obtain and process information fairly
- Keep it only for one or more specified, explicit and lawful purposes
- Use and disclose it only in ways compatible with these purposes
- Keep it safe and secure
- Keep it accurate, complete and up-to-date
- Ensure that it is adequate, relevant and not excessive
- Retain it for no longer than is necessary for the purpose or purposes
- Give a copy of his/her personal data to an individual, on request

A minimum standard of security would include the following:

Data Commissioners Recommendations	MindaClient Compliance
access to central IT servers to be restricted in a secure location to a limited number of staff with appropriate procedures for the accompaniment of any non-authorised staff or contractors;	Only relevant people should be given access to the MindaClient database
access to any personal data within an organisation to be restricted to authorised staff on a 'need-to-know' basis in accordance with a defined policy;	The Administrator of MindaClient within your organisation can decide which members of staff have access to MindaClient
access to computer systems should be password protected with other factors of authentication as appropriate to the sensitivity of the information;	Access to MindaClient is always through a secure Username & Password. Each user can and should regularly update their own password
information on computer screens and manual files to be kept hidden from callers to your offices;	Procedure to be put in place locally to ensure compliance. Additionally, MindaClient automatically logs out if not used for a period.
back-up procedure in operation for computer held data, including off-site back-up;	MindaClient is backed up, including off-site back-up
all reasonable measures to be taken to ensure that staff are made aware of the organisation's security measures, and comply with them;	Staff should be made aware of procedures internally
all waste papers, printouts, etc. to be disposed of carefully;	Procedure to be put in place locally to ensure compliance.
a designated person should be responsible for security and for periodic reviews of the measures and practices in place.	Procedure to be put in place locally to ensure compliance.