## 1   ForestSafe SaaS Service details

1.1   Service Description

ForestSafe is a privileged identity management system used today to manage the Administrator passwords of 65,000 computers by the UK largest bank.

It has completely secured their password infrastructure since 2007, and is used by support staff when they occasionally need elevated rights to perform their work. All access is audited and controlled.

1.2   Functional
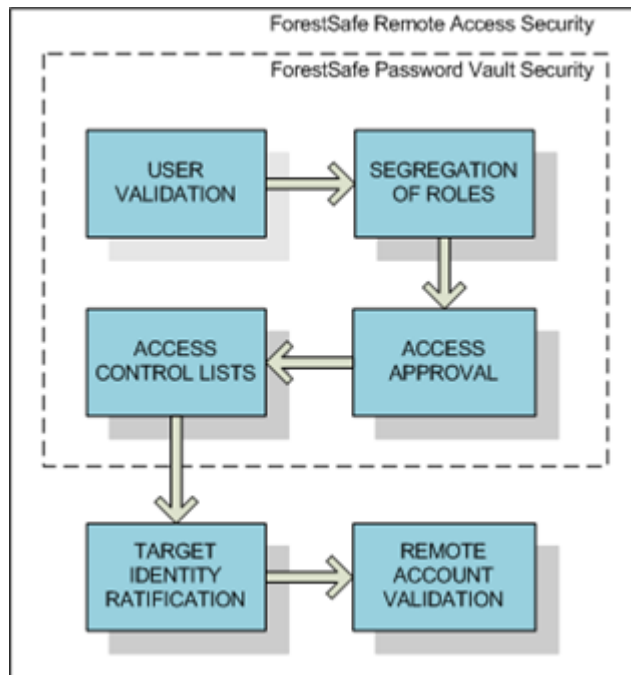
1. ForestSafe is launched through a Web browser on the user's desktop
2. Their logged in credentials are scrutinised by the ForestSafe Service.
3. It prompts to re-enter their domain password
4. If authorised, the ForestSafe Web application is launched in their browser.
5. The user sees only what they have been configured to see. This is setup during system installation and configuration.

1.3   Non Functional

ForestSafe is a background security system automatically 'securing' passwords of high risk accounts, until they are needed by staff. Some examples why staff may need to retrieve a high risk account password are:

1) Launch a remote terminal as an Administrator or ID 0 account, to a remote machine for support.

2) Retrieve local administrator password to allow a support user to install a network card.

3) Retrieve service account password, to install a secondary service under the same account.
4) Retrieve SAP* password to manage a SAP system.
5) Launch a password free Lotus Domino administrator session.

All ForestSafe SaaS instances are unique to ensure complete security and segregation. The system supports password Self Service and also Approval layer.

(*See the ForestSafeAdministratorGuide.pdf for more information*)

1.4 Scope

The scope of the service covered by this service definition includes:

- *Rackspace managed SaaS hosting (backbone)*
- *ForestSafe SaaS instance*

1.5 Roles and Responsibilities

Customer will nominate a primary and secondary named contact who will be enabled to log incidents 24x7 on the website:

http://www.eesm.com/Support/ticketing.php

1.5.1 Training

A Half a day's training course is available for End users e.g. Service Desk and IT Security. Training is charged at £220 per hour, for unlimited number of students.

1.6 Information assurance –

1.6.1 Impact Level (IL) at which the Service is accredited to hold and process information

The SaaS hosting company supporting the service, **Rackspace** has IL1 accreditation.

1.6.2 Whether you hold a suitably scoped ISO27001 certificate for this G-Cloud Service

Rackspace:
http://www.rackspace.co.uk/sites/default/files/Rackspace_ISO27001_Cert A6_ED2015.pdf

Entarian Limited:
"Awaiting implementation record"

1.7 Service Times

The (Service Name) is available to customers at the following times:

Mon – Fri	24 Hours
Saturday	24 Hours
Sunday	24 Hours
Bank Hols	24 Hours
Exceptions	None

All times are quoted in UK hours (GMT and BST).

1.8 Support Arrangements

1.8.1 Incident logging

Incidents can be logged by nominated contacts on the website

Escalation process is triggered by incident logging website unavailability or failure to respond within 48 hours

The escalation process is telephoning 0203 514 0910 and requesting support

1.8.2 Resolver Groups

Hardware support is available:

	Infrastructure Support
Mon – Fri	24 Hours
Saturday	24 Hours
Sunday	24 Hours
Bank Hols	24 Hours
Exceptions	None

Application support is available:

	Core Support Times	On Call Support
Mon – Fri	09:00 – 18:00	18:00 – 08:30
Saturday	No Support	24 Hours
Sunday	No Support	24 hours
Bank Hols	No Support	24 Hours

1.8.3 Out of Hours arrangements

Infrastructure and application on call support is available for high impacting major incidents only. The decision to invoke out or hours support will be made by the primary contact only.

Monday –Friday	04:00 - 06:00 hrs

1.9 **Maintenance Window**

A maintenance windows enable planned service interruptions so that essential maintenance, repairs, housekeeping or service upgrades can be carried out. During each maintenance window ForestSafe may not be available to the users (or describe effect/impact on users). Such windows will be raised and notified through the IT Change management process and notification and approval will include but not be confined to the signatories in Section 1.1.

The following maintenance windows apply:

Maintenance Task	Frequency	Duration
Windows Server Maintenance	24 per year	22:00 – 06:00 Weekends

1.10 **Service Targets**

1.10.1 Service Availability

ForestSafe SaaS has a target availability of 100% uptime and 1 hour guaranteed replacement for hardware failures for server failure.

1.10.2 Degraded Service / Usability

Performance of ForestSafe SaaS is monitored. Monitoring of the service for 6 months shows that it generally takes less than 2 seconds to access the home pages of the reference sites used (internal Site). This timing will be used as a basis for performance measuring when dealing with any service issues involving degraded service.

1.10.3 Service Reliability

ForestSafe has an MTBSI of 3 years over 3 Years at Lloyds Banking Group, managing 65,000 computers from the LBG internal VMware cloud.

1.10.4 Backup/Service Continuity/Disaster Recovery

ForestSafe SaaS instances are backed up and off-sited automatically.

Rackspace RTO target of 1 hour

1.10.5 Data Centres

Where appropriate, customer will be given a geographical choice of data centre

1.11 **Security**

Rackspace is an accepted government supplier. (*See Rackspace Service Definition*)

ForestSafe leverages Microsoft best practice Kerberos security. (*See ForestSafeSecurity.pdf on request*)

Traffic between customer and through ForestSafe SaaS instance Firewall is via persistent secure VPN channel. This is industry standard approach for SaaS security.

1.12 Change Procedure

1.12.1 Additional/Removed Servers and Workstations

Windows machines in Active Directory are **automatically managed**, through pre-configured policy.

Unix and Windows Workgroups machines can be automatically or manually imported depending on pre-configured policy.

1.12.2 Additional/Removed Users

Additional end users of the system will be **automatically configured**. ForestSafe maps end user to functional groups through Active directory membership. No client software or agents.

1.12.3 Additional/Removed End User Groups

ForestSafe Administrator will manually make a configuration change (business as usual).

1.12.4 Additional/Removed Managed accounts

ForestSafe Administrator will make a configuration change.to the system, (business as usual).

1.12.5 On-boarding and Off-boarding by consumers

OnBoarding

1. Department completes **ForestSafeWhiteBook** system configuration template
2. *Forest SaaS server instance joins Windows Domain and ForestSafe Saas service set to run with restricted privilege on the domain (see ForestSafeServiceConfiguration.pdf)**
3. *Department creates DNS entry Web application and Service Principal Names for Kerberos security from the WhiteBook template**
4. Entarian configure the system from **ForestSafeWhiteBook** template

*Only required if a new ForestSafe SaaS instance is commissioned – see 2.14 charging

Provisioning Time

Step1: The WhiteBook system configuration template must be completed and approved by all stake holders.

Step2: It takes ½ day /1 day to implement a WhiteBook configuration and carry out sign off testing.

Off-Boarding

1. All managed local account passwords set to same value and made available to primary named contact.
2. All managed Shared account passwords are retrieved and made available to the primary named contact.
3. ForestSafe SaaS Instance is removed from customer AD and all instances decommissioned from Rackspace Cloud.
4. Department delete DNS entry and SPNs.

1.12.6 On-boarding and Off-boarding by customer

See consumer.

1.12.7 Data restoration / service migration

Not applicable

1.13 Capacity Management

ForestSafe was designed by a team including system management capacity planning consultants. It is designed to scale.

The (service) has been measured taking 100MB RAM managing 67,000 computers at our largest customer. Each password reset measured 4KB of bandwidth. Resetting 67,000 computer passwords took 268Mb bandwidth in total.

By default each ForestSafe SaaS single-tier instance is allocated 2GB RAM with 2 cores running R2 2008 Server and Microsoft SQ Express or Standard depending on the size of the infrastructure.

There are many ways to increase capacity

1. The Server running ForestSafe can migrated up to 8 cores
2. ForestSafe can be spread from single tier to 3-tier after install.
3. Several Web Servers instances can be used with DNS switch for load balancing.

Additional capacity will be made available through Rackspace cloud and is a simple re-configuration.

Entarian do not derive income from the cloud hosting, all costs are passed directly to Rackspace. Please check Rackspace list prices for additional capacity and Entarian can give estimates accordingly.

1.14 **Charging**

1.14.1 ForestSafe SaaS instance charges

ForestSafe cost is Cloud Hosting Cost + ForestSafe Licence cost. A ForestSafe licenses for a single Windows or UNIX computers costs £2 per year.

The prices in this table include the cost of the cloud hosting.

Data centre tiers	ForestSafe computer licences included	Capacity	MS SQL Server Express	MS Server Standard
1	300	5000 computers	£2,500	£7,500
3	900	Unlimited	£9,000	£13,000

Cost includes unlimited support

Cost increases annually by RPI as published by the statistics office of the government.

Volume discounts are available:
- Volumes over 10,000 computers = 25% discount,
- Volumes over 60,000 computers = 40% discount,
- Volumes over 100,000 computers = 77% discount.

Other discounts are available:

Customer hosting locally, and not using SaaS, pay £6 per computer per year, as there is no cloud hosting cost.

Customers sharing the ForestSafe cloud infrastructure can make savings on the hosting costs

Consulting

Entarian consultants are available during normal service hours, by phone or site visit at a cost of £220 per hour plus expenses.

1.14.2 Trial Service

A 30 day trial of ForestSafe **Express** service can be downloaded by clicking here

http://www.eesm.com

1.14.3 Ordering and invoicing process

Intention to purchase with details of configuration is sent to **sales@eesm.com**

Entarian will send an invoice. Payments can be made by cheque or BACS

Cheque

Entarian Limited

30 City Road

London

EC1Y 2AB

BACS

Entarian Limited

Sort code   On Request

Account   On Request

1.14.4 Aggregated billing

We can aggregate billing from multiple cost-centres if required.

1.14.5 Incentives & Penalties:

Service credits will be awarded based on:

Hardware failure is the responsibility of Rackspace, see their SLA.

http://www.rackspace.com/cloud/legal/sla/

- ForestSafe System failure – Entarian will refund licence cost for duration of outage.

2   EXCEPTIONS

2.1   Thresholds

The Service Targets defined in section 1.10 of this Service definition cannot be guaranteed if any of the following thresholds are exceeded.

Measure	Threshold
Number of computers managed by a ForestSafe SaaS System	No more than 300,000

When a threshold is exceeded this will trigger a review by SLM of this service, and it's

SLA and OLAs, see capacity planning section for options.

3 Management reporting

3.1 Reporting

ForestSafe has a system for generating management reports. In addition the product has a real-time management dash board for monitoring the state of the managed infrastructure.

4 Appendices

4.1 Glossary

Not required

4.2 Component OLAs & Underpinning Contracts

Rackspace Cloud SLA – taken from
http://www.rackspace.com/cloud/legal/sla/

The Rackspace Cloud provides the same guaranty for Cloud Servers™ as Rackspace does for traditional hosted servers. Specifically:

4.2.1 Network

We guaranty that our data center network will be available 100% of the time in any given monthly billing period, excluding scheduled maintenance.

4.2.2 Data Center Infrastructure

We guaranty that data center HVAC and power will be functioning 100% of the time in any given monthly billing period, excluding scheduled maintenance. Infrastructure downtime exists when Cloud Servers™ downtime occurs as a result of power or heat problems.

4.2.3 Cloud Server Hosts

We guaranty the functioning of all cloud server hosts including compute, storage, and hypervisor. If a cloud server host fails, we guaranty that restoration or repair will be complete within one hour of problem identification.

4.2.4 Migration

If a cloud server migration is required because of cloud server host degradation, we will notify you at least 24 hours in advance of beginning the migration, unless we determine in our reasonable judgment, that we must begin the migration sooner to protect your cloud server data. Either way, we guaranty that the migration will be complete within three hours of the time that we begin the migration.

4.2.5 Credits

If we fail to meet a guaranty stated above, you will be eligible for a credit. Credits will be calculated as a percentage of the fees for the Cloud Servers™ adversely affected by the failure for the current monthly billing period during which the failure occurred (to be applied at the end of the billing cycle), as follows:

Network: Five percent (5%) of the fees for each 30 minutes of network downtime, up to 100% of the fees;

Data Center Infrastructure: Five percent (5%) of fees for each 30 minutes of infrastructure downtime, up to 100% of the fees;

Cloud Server Hosts: Five percent (5%) of the fees for each additional hour of downtime, up to 100% of the fees;

Migration: Five percent (5%) of the fees for each additional hour of downtime, up to 100% of the fees.

Definitions: For purposes of this Service Level Guaranty:

- "cloud server" means your unique virtual machine instance;

- "cloud server fees" means the fees for your Cloud Servers™ for the monthly billing period in which the failure occurred and includes monthly virtual machine instance and bandwidth charges;

- "cloud server host" means the physical server which hosts your cloud server;

- "data center network" means the portion of The Rackspace Cloud network extending from the network egress point of your cloud server host to the outbound port of the data center border router;

- "power" includes UPSs, PDUs and cabling, but does not include the power supplies in cloud server hosts;

- "scheduled maintenance" means maintenance that is announced at least ten business days in advance, and that does not exceed sixty minutes in any calendar month.

4.2.5.1 Limitations.

You are not entitled to a credit if you are in breach of your services agreement with The Rackspace Cloud™ (including your payment obligations to us) until you have cured the breach. You are not entitled to a credit if downtime would not have occurred but for your breach of your agreement with The Rackspace Cloud or your misuse of Cloud Servers™ system.

To receive a credit, you must contact your The Rackspace Cloud account team within thirty (30) days following the end of the downtime. You must show that your use of the Cloud Servers™ was adversely affected in some way as a result of the downtime to be eligible for the credit.

This Service Level Guaranty is your **sole and exclusive** remedy for Cloud Servers™

unavailability.

Notwithstanding anything in this Service Level Guaranty to the contrary, the maximum total credit for the monthly billing period, including all guaranties, shall not exceed 100% of your fee for that billing period. Credits that would be available but for this limitation will not be carried forward to future billing periods.

This Service Level Guaranty is part of your Agreement with The Rackspace Cloud, along with The Rackspace Cloud™ Terms of Service and the AUP, and is subject to the terms and conditions stated in those documents.