

Introducing

ForestSafe

Entarian Limited 2014

Enterprise level local and shared account password management for Windows, Unix, Cisco, Mainframe and all devices supporting SSH or telnet. System Account provisioning and Secure Remote Access.

Make any account password, custom application or windows service unique, or synchronise any set of account passwords. Temporary and permanent provisioning of system accounts with common or unique passwords.

Give support staff a fully audited, controlled, secure Terminal access to any computer, and simple reporting functions to meet SOX compliance

 LIPPO CENT

1

The problem

All local Windows administrator passwords are identical by default.

If a virus affects a single computer, and gains access to it's IP neighbour, it spreads to every computer.

Root and administrator passwords that cannot change allow unaccountable administrator. A computer administrator with knowledge of a "never changing" password, can wreak havoc with your systems, and may have simply been trying to help.

Organisations have reported losing weekends of computer time, due to an administrator applying a fix, unknown to anyone but themselves having bypassed the approval mechanism.

Companies are failing to respect compliance standards unless they manage their unmanaged accounts and may face financial penalties.

Password management is missing from the list of infrastructure management services e.g. availability, software management. Yet it is the most critical service of all.

2 The solution

ForestSafe is a policy driven highly scalable, highly granular, high availability 3-tier Enterprise Privileged Identity Management system, available as local data center installation or Rackspace Managed SaaS instance.

Also integrated is a secure SSH/Telnet/Remote terminal Web interface, you need no other SSH client tools. And there are several levels of security.

Control and monitor all your remote access. See a real time Dashboard of all system activity.

Monitor the logon of released passwords and force password expiry if not used in time. Continually test all managed account passwords.

ForestSafe is an agent-less automated solution.

For more information:

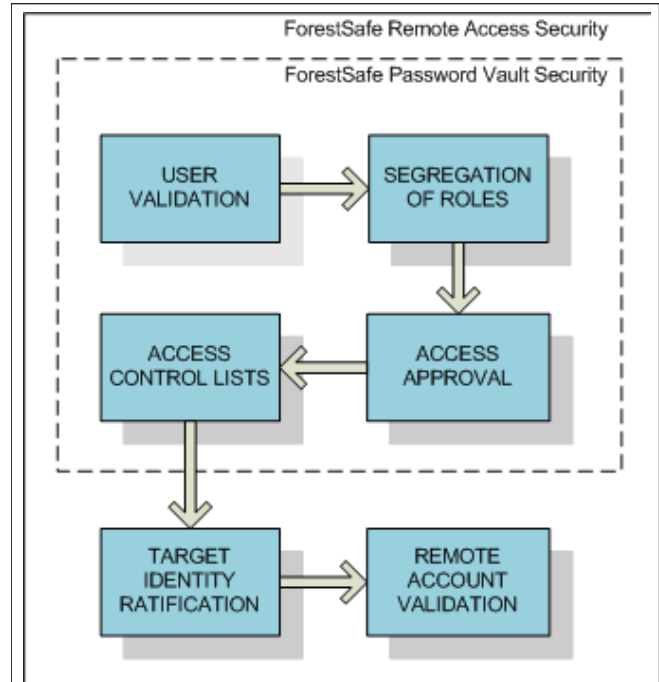
Please visit our web site:

<http://www.eesm.com>

UK Government customers visit:

<http://govstore.service.gov.uk/cloudstore/forestsafe-privileged-computer-account-management4-g4-0478-201>

ForestSafe is used by Lloyds Banking Group to manage the local administrator passwords of 67,000 Windows Servers and Workstations.



1. User Validation is the doorway to the remote access.

2. Segregation of roles enforces partitions exist between the ForestSafe administrator roles.

3. Access Approval is available to apply an extra layer of authority between users and the hosts that are allowed to access remotely.

4. Access Control Lists define which hosts Administrators are allowed to access, and also which user accounts they logon with.

5. Target Identity ratification is a final security check, to prevent "Man in the Middle" attacks

6. Remote Access Validation is the final doorway to remote system.

3 Installation

Local installation



ForestSafe is available as a local single or 3-Tier and HA installation. It requires Windows 2008 R2 servers.

The system has an extremely light footprint and can be installed on existing servers with no interruption to existing services.

Software as a Service



ForestSafe is installed on Rackspace Windows 2008 R2 instance/s.

The Windows server instance joins the department Windows Domain to allow trusted authentication from the ForestSafe Web interface.

Rackspace is authorised to supply cloud computer services to the UK government.