# CONTENTS

<table>
<thead>
<tr>
<th>Topics</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>OneGate Components</td>
<td>4</td>
</tr>
<tr>
<td>OneGate Gateway</td>
<td>4</td>
</tr>
<tr>
<td>OneGate Management Console</td>
<td>4</td>
</tr>
<tr>
<td>OneGate OS Console</td>
<td>4</td>
</tr>
<tr>
<td>OneGate Access Modes</td>
<td>4</td>
</tr>
<tr>
<td>Preparing for Proof of Concept</td>
<td>5</td>
</tr>
<tr>
<td>OneGate Availability</td>
<td>5</td>
</tr>
<tr>
<td>Deployment</td>
<td>5</td>
</tr>
<tr>
<td>Physical / Virtual Hardware Requirements</td>
<td>6</td>
</tr>
<tr>
<td>Evaluation License Requirements</td>
<td>6</td>
</tr>
<tr>
<td>Integration Requirement</td>
<td>7</td>
</tr>
<tr>
<td>Directory Services Integration</td>
<td>7</td>
</tr>
<tr>
<td>Firewall Changes</td>
<td>7</td>
</tr>
<tr>
<td>Proof of Concept Checklist</td>
<td>8</td>
</tr>
<tr>
<td>Propalms OneGate Technical Specifications</td>
<td>9</td>
</tr>
</tbody>
</table>
## ONEGATE COMPONENTS

### ONEGATE GATEWAY

This is the core gateway component of the solution. The OneGate gateway is built of web server, SSL engine, session manager, policy manager and policy database. OneGate gateway is developed as a high performance and scalable service written in C and C++ languages and it runs on a hardened Linux based OS. Mentioned below are components of OneGate gateway:

- Propalms OneGate core server: Proprietary OneGate server engine developed by Propalms
- Propalms OS: CentOS 5.0 Linux distribution (hardened), Kernel 2.6.
- Apache web server: To serve management pages and portal
- Propalms Configuration database: Configuration database
- OpenSSL: The SSL engine of Propalms OneGate is based on the open source OpenSSL library.

### ONEGATE MANAGEMENT CONSOLE

Propalms OneGate provides a built-in web based management console interface. Through the management console, a OneGate administrator can do complete OneGate system management and maintenance. The OneGate management console is available only to certificate based logins of security officer and administrators.

### ONEGATE OS CONSOLE

OneGate OS Console is the Linux menu driver interface developed by Propalms for low level maintenance of the OneGate appliance. This console is visible when a console is connected to the OneGate appliance. Using the OS Console interface administrators can set networking parameters, can reinstall the firmware and get access to full CLI mode of Propalms OS.

### ONEGATE ACCESS MODES

OneGate’s Access Modes are the different ways that users can login to Propalms OneGate and can access the corporate network resources. These modes are:

1. **OneGate Portal**: Propalms OneGate comes as a web portal for remote users. Users can use any browser of their choice and can login into Propalms OneGate and access network resources. The portal is enabled with a Java based plug-in that provides the enhanced security to users as well as enabling access to client-server based applications. Users logging into the web portal can access web based application as well as client-server based applications. Along with this, the web portal is enabled with Java based terminal emulators that provides a set of ready to use applications to a mobile users such as FTP, SSH, Telnet, RDP, VNC and file share.

2. **OneGate Desktop Client**: Propalms OneGate comes with a desktop client that a user can install on their Windows PC, Linux or Mac OS desktop removing the need to go to the browser every time. A desktop client gives much faster connectivity to the user and is very helpful for users who stay connected to OneGate for longer times. Desktop client has an application launcher that lists all the applications the user has access to. This enhances the user experience and reduces the training time needed to train the users to access the resources over OneGate.

3. **OneGate Mobile Clients**: Propalms provides mobile clients for smart phones and tablets. The mobile client is called Propalms Universal Client and is currently available for iPad, iPhone and Android based devices. Propalms Universal Client is a single client that can connect to different Propalms solutions and delivers applications,
desktops and network services. Currently only Propalms TSE, Propalms Pano VDI and RDP based applications are supported over Propalms Universal Client.

Shown below is a comparison of the different access modes:

<table>
<thead>
<tr>
<th>Feature</th>
<th>ONEGATE Web Portal</th>
<th>Desktop Client</th>
<th>Mobile Client</th>
</tr>
</thead>
<tbody>
<tr>
<td>Platform Supported</td>
<td>Windows (Linux/MAC Support by Q1 2013)</td>
<td>Windows MAC OSX Lion / Snow Leopard Linux: all flavors</td>
<td>iPad: 4.0/5.0 iPhones Android: 2.2 and higher</td>
</tr>
<tr>
<td>Browser Supported</td>
<td>Internet Explorer 7.0 and higher Firefox Chrome</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Applications Supported</td>
<td>Web, Thin applications, Client-Server, Any TCP/UDP application</td>
<td>Web, Thin applications, Client-Server, Any TCP/UDP application</td>
<td>Propalms TSE, Propalms Pano VDI, RDP</td>
</tr>
<tr>
<td>Advantage</td>
<td>Seamless access, Ease of use, Zero training involved</td>
<td>Seamless access, Ease of use, Power users loves it</td>
<td>Access over tablets, smartphones</td>
</tr>
<tr>
<td>Java Requirement</td>
<td>Requires Java</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Admin Rights Requirements</td>
<td>Require admin rights on first use only</td>
<td>Require admin rights on first use only</td>
<td>-</td>
</tr>
<tr>
<td>Upgrades</td>
<td>Self-upgrades</td>
<td>Self-upgrades</td>
<td>Via AppStore/Market</td>
</tr>
</tbody>
</table>

**PREPARING FOR PROOF OF CONCEPT**

**ONEGATE AVAILABILITY**

Propalms OneGate is available as a software installer ISO image. This single click integrated ISO image installs both Propalms OS and Propalms OneGate on any custom hardware. The installer ISO can be downloaded from the Propalms Website (http://www.propalms.com).

Propalms OneGate is also available in Open Virtualization Format (OVF) which is an open standard for packaging and distributing virtual appliances to be run in virtual machines. The Propalms OneGate Virtual Appliance has been verified with VMware ESXi. The Virtual Appliance is downloadable from the Propalms Website (http://www.propalms.com). Simply extract the image file and import directly into your VMware environment and you are ready to go.

Propalms OS is a CentOS based platform, hence any hardware that supports the Linux distribution is supported by Propalms OS. Propalms OS is available in both 32-bit and 64-bit versions.

The functionalities of the OneGate platform are the same irrespective of the underlying platform.

**DEPLOYMENT**

For a Proof of Concept (PoC), we suggest a close to real life deployment as suggested in diagram.

Propalms OneGate can be setup in the DMZ network or connected to LAN switch. Only one of the interfaces of OneGate gateway needs to be connected. This is the simplest deployment and is recommended for production deployment also.
Create NAT for port 443 and DMZ/LAN IP address of OneGate Server

OneGate in DMZ or LAN

Active Directory

Application Servers

PHYSICAL / VIRTUAL HARDWARE REQUIREMENTS

Shown below are some example server hardware requirements and approximate number of concurrent users supported.

<table>
<thead>
<tr>
<th>Item</th>
<th>Up to 50 Users</th>
<th>100 Users</th>
<th>250 Users</th>
<th>500 Users</th>
<th>1000 Users</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU</td>
<td>Any CPU 2.0 GHz</td>
<td>Any standard Dual core CPU 2.0 GHz</td>
<td>Any standard Dual core CPU 2.0 GHz</td>
<td>Xeon Quad Core entry level processor 2.0 GHz</td>
<td>Xeon Quad Core processor 2.4 GHz</td>
</tr>
<tr>
<td>RAM</td>
<td>2 GB</td>
<td>2 GB</td>
<td>4 GB</td>
<td>8 GB</td>
<td>16 GB</td>
</tr>
<tr>
<td>Hard disk Space</td>
<td>4 GB minimum</td>
<td>4 GB minimum</td>
<td>50 GB minimum</td>
<td>100 GB minimum</td>
<td>160 GB minimum</td>
</tr>
<tr>
<td>Network Card</td>
<td>100 Mbps</td>
<td>100 Mbps</td>
<td>2 x 1 Gbps</td>
<td>2 x 1 Gbps</td>
<td>2 x 1 Gbps</td>
</tr>
</tbody>
</table>

EVALUATION LICENSE REQUIREMENTS

When Propalms OneGate is freshly configured, a 5 user evaluation license valid for 30 days is available by default. To test more users or to extend the evaluation period simply ask for an evaluation license key by emailing info@propalms.com.
INTEGRATION REQUIREMENT

DIRECTORY SERVICES INTEGRATION

Propalms OneGate can integrate with existing Active Directory infrastructure for applying authentication and authorization to existing users. The following details are needed to integrate active directory with OneGate:

1. IP address/hostname of domain controller
2. Distinguished Name (DN) of a domain user who is member of ‘Account Managers’ group. i.e. the user should have account management rights
3. Password of this user
4. Search base in domain controller
5. If SSL is enabled on active directory or not
6. If user must be able to change their domain password via OneGate, SSL MUST be enabled on active directory.

FIREWALL CHANGES

Propalms OneGate must be available to users on a public IP address so that users outside the office network can access the OneGate services. The following configuration change is required on the firewall for accessing Propalms OneGate over the internet

“A NAT rule needs to be created on the firewall to allow HTTPS traffic (Port 443) from outside world to Propalms OneGate gateway’s internal IP address.”

In case Propalms OneGate is deployed in DMZ, necessary firewall configuration should be created so that traffic coming from Propalms OneGate gateway IP address should be allowed to access the application servers deployed in other network segments (like LAN).

“Traffic coming from Propalms OneGate for the internal application servers and network segments must be permitted on firewall on DMZ port.”

IMPORTANT: It is recommended to refer to Propalms OneGate Quick Start Guide and Propalms OneGate Administration Guide for detailed information.

Download Latest Propalms ONEGATE Documents from here
http://www.propalms.com/download/documentation.php#OneGate
## PROOF OF CONCEPT CHECKLIST

Use this list as a brief checklist to track and record your POC of Propalms OneGate. Not all steps are mandatory.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Check</th>
</tr>
</thead>
<tbody>
<tr>
<td>Propalms ONEGATE OS installed on hardware</td>
<td></td>
</tr>
<tr>
<td>LAN IP address assigned to Propalms ONEGATE</td>
<td></td>
</tr>
<tr>
<td>Propalms ONEGATE bootstrap process run</td>
<td></td>
</tr>
<tr>
<td>First security officer registered</td>
<td></td>
</tr>
<tr>
<td>First security officer enrolled</td>
<td></td>
</tr>
<tr>
<td>Logged into ONEGATE management console</td>
<td></td>
</tr>
<tr>
<td>Moved ONEGATE from Configuration mode to Run Mode</td>
<td></td>
</tr>
<tr>
<td>Created another security officer account as backup</td>
<td></td>
</tr>
<tr>
<td>Integrated with external authentication server (AD/RADIUS)</td>
<td></td>
</tr>
<tr>
<td>Applications created on ONEGATE</td>
<td></td>
</tr>
<tr>
<td>Application groups created on ONEGATE</td>
<td></td>
</tr>
<tr>
<td>Access control for application access created on ONEGATE</td>
<td></td>
</tr>
<tr>
<td>Tested login to ONEGATE via web portal</td>
<td></td>
</tr>
<tr>
<td>Tested login to ONEGATE via desktop client</td>
<td></td>
</tr>
<tr>
<td>iPad/Android client tested</td>
<td></td>
</tr>
<tr>
<td>Configured SMTP settings</td>
<td></td>
</tr>
<tr>
<td>Tested application access for</td>
<td></td>
</tr>
<tr>
<td>- HTTP based application</td>
<td></td>
</tr>
<tr>
<td>- HTTPS based application</td>
<td></td>
</tr>
<tr>
<td>- RDP server</td>
<td></td>
</tr>
<tr>
<td>- VNC server</td>
<td></td>
</tr>
<tr>
<td>- Email access</td>
<td></td>
</tr>
<tr>
<td>- Microsoft Exchange Server</td>
<td></td>
</tr>
<tr>
<td>- File share</td>
<td></td>
</tr>
<tr>
<td>- Any other applications</td>
<td></td>
</tr>
<tr>
<td>Configure certificate based authentication for local database users</td>
<td></td>
</tr>
<tr>
<td>Tested endpoint security for checking AV/FW/AS</td>
<td></td>
</tr>
<tr>
<td>Tested Device ID authentication</td>
<td></td>
</tr>
<tr>
<td>Tested endpoint control policy by blocking Internet, etc.</td>
<td></td>
</tr>
<tr>
<td>Tested user settings backup and restore</td>
<td></td>
</tr>
<tr>
<td>Tested remote meeting feature</td>
<td></td>
</tr>
<tr>
<td>Tested client preference control feature</td>
<td></td>
</tr>
<tr>
<td>Tested One time password authentication</td>
<td></td>
</tr>
<tr>
<td>Tested network information hiding feature</td>
<td></td>
</tr>
</tbody>
</table>
MANAGEMENT
- Web based management console
- Dashboard with graphical reporting
- Menu driven console interface for system configuration
- Wizard driven installation procedure
- Self-signed certificate generation
- CLI
- Delegated administration
- Certificate based strong authentication for administrators
- Auto checking for configuration errors
- Online License service
- Inline help

APPLICATION SUPPORT
- All web based, TCP and UDP based client-server applications
- Windows file shares and drive mapping
- Dynamic port based applications
- Publish Subnet or IP Range for network access
- Special support for RDP virtual channels
- Application server load balancing
- Session caching for load balanced applications
- Per application based compression switch
- My Desktop and Files for direct personal desktop and file access
- Propalms TSE hosted applications
- Propalms VDI hosted desktops

AUTHENTICATION FEATURES
- Authentication based on user identity, endpoint identity, endpoint trust level
- Multiple user authentication options: static passwords, client certificates, external two factor authentication solutions
- Local database with full customization per user, password policies, password reset support
- Fully integrated client-certificate based two factor authentication server with automatic CA and certificate provisioning
- Email based user provisioning
- Authentication method based application access control
- Integrates with AD/LDAP/RADIUS
- Automatic fetching of group information from AD/LDAP/RADIUS
- Support for multiple authentication servers with cascading mode
- Support for external authorization servers
- Integrated OTP based Two factor authentication solution based on SMS/Email/Hardware/Voice/PKI tokens

AUTHORIZATION FEATURES
- Publish applications rather than subnet or network
- Simple access control mechanism
- Access control based on
  - Device identity and profile
  - User Authentication method
  - User Role
- Dynamic policy evaluation based on run time information about device, authentication method and user role
- Display of allowed applications and availability of the application server to users
- Time based restriction policies
- Auto-detection of applications running in corporate network
- Scheduled account expiry
- Block specific groups

AUDITING FEATURES
- Complete reporting of user logons and activity
- Information logged includes
  - Time of access
  - Username
  - MAC Address of endpoint
  - IP address of endpoint
  - Application accessed
  - Device profile
- Detailed logging of endpoint security scans results
- Extract logs in CSV format for feeding to third part report generation
- Search logs
- Auto-archiving of logs
- Monitor and disconnect live users

ENDPOINT MANAGEMENT
- Support for checking for antivirus, firewall and antispyware products
- Real time status check for
  - Last update time
  - Real time protection check
- Support for checking for MAC ID and IP address
- Application control based on device profile
- Mandatory profile for non-avoidable policy checks on all endpoints
- Quarantine profile for devices that fails all other profile
- Option to block endpoints that fails to comply to required policies or option to allow them to login by putting them in quarantine profile
- Login control based on device signature
- Kill existing TCP connections on user machine
- Block Internet and restrict incoming connection policy
- Block access via proxy server policy

DEPLOYMENT SCALABILITY
- Scalable to thousands of users
- Active-Active N+1 cluster
- VPN connections load balancing, multiple algorithms
- Application connection load balancing can distribute the connection for a specific application across multiple app servers in the LAN based on round robin function
- Session persistence: Users do not need to re-authenticate
- ISP load balancing for incoming connections
- Client side failover using Alternate gateways
- 64-bit hardware support

ACCESS SECURITY FEATURES
- SSL 3.0 and TLS 1.0
- Encryption: Strongest available: DES, 3DES, AES(256), RC4
- Authentication: MD-5, SHA-1, RSA 1024, RSA 2048
- 4096 bit RSA key CA certificate support
- Internet network masking and IP address/hostname mangling
- Application level gateway and not layer 2 bridging
- Hardened gateway operating system

ACCESS MODES
- Multiple access modes:
  - VPN portal with java applications
  - Full access client for desktops
  - Kiosk based access mode for non-admin access
  - No configuration required on end user machines
  - Client platforms supported
    - Windows 98/XP/Vista/Windows7/Windows 8
    - Windows server 2003/2008/2012
    - Linux OS
    - MAC OS X PPC/Intel 10.4 and above
    - iPad / Android Access
  - Site to site access

GATEWAY FEATURES
- Runs on hardened Linux based platform
- Menu driven console interface for easy configuration
- Can run on any standard or custom hardware
- Virtual server for using VPN as HTTPS proxy
- Runs on virtualization platforms from VMWare, XenServer, Hyper-V