

Trusted Identities, Managed Access

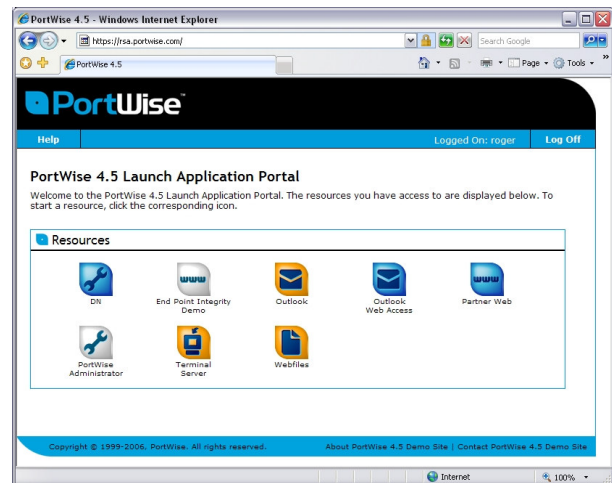
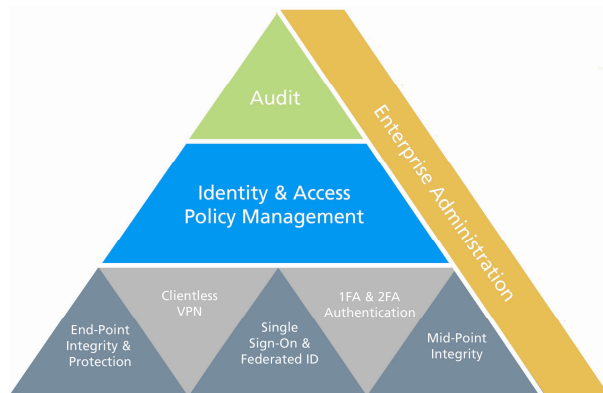
Implementing an Identity and Access Management Strategy for the Mobile Enterprise

INTRODUCTION

Whether you are looking to securely connect remote employees to your applications and data, secure online business relationships, or deliver convenient identity and access solutions to your end-customers, implementing an Identity and Access Management Strategy for the Mobile Enterprise is a key objective for many of today's enterprises. Most organizations have taken a piecemeal approach to deploying Mobile Identity and Access Management such as VPNs, Authentication, or Single Sign-On products but with the evolving security threat and spiraling costs of managing security, many are looking to deploy a smaller number of secure solutions rather than more security solutions. Whether your requirement is simply for a leading clientless VPN or authentication product, or whether you need a complete entry-to-exit solution for your mobile enterprise, the all-software PortWise approach offers a comprehensive, integrated and secure way to enable any user, to connect to specific application and data resource, from any device, in any location.

uses standard Web browsers (i.e. Internet Explorer, Firefox, or Safari) for access. This results in users having access from any location and any device. User's still have access to all applications and data through an encrypted connection. By not having to install any software deployment becomes easy and administration a breeze.

- **Strong Encryption** – By using industry standard encryption, user's data and activities are safe from hackers. PortWise uses 128 or 256bit encryption.
- **User-Friendly Portal** – PortWise uses a device friendly Portal to present a users applications and resources. Using reduced sign-on allows the user to log on once and have access to everything in the Portal. The Portal auto-detects device being used and adapts the Portal accordingly.



CLIENTLESS VPN

Many organizations start their mobile access strategy with an SSL VPN.

Securing communication from a user's device to the applications and data being accessed is critical in ensuring a safe and productive working environment. PortWise helps optimize the user experience with the following:

- **Clientless** – PortWise software SSL VPN removes the need to install proprietary software on a device for access, but

- **Support for EVERY Application** – PortWise supports all applications including Web-based, client/server, mainframe, terminal server, bi-directional (VoIP, online collaboration tools), and file servers. As a software solution, the PortWise SSL VPN is uniquely customisable to support any class of application.
- **Scalability & Performance** – The PortWise SSL VPN solution uses multiple access points to ensure almost infinite scalability and performance without the use of hardware accelerator cards
- **Built-in Business Continuity/Highly Availability** – Each PortWise Access Point can be mirrored to an unlimited amount of servers at no additional cost. This guarantees 24x7 access.



AUTHENTICATION

Identities can be faked or stolen, which is why organizations must have bullet-proof authentication in place to ensure sensitive data is not breached. PortWise provides strong authentication with the following benefits:

- **Mobile Two-Factor Authentication (MobileID)** – By using a consumer device the user already owns, such as a mobile phone, PDA, or BlackBerry, to generate a unique one-time password (OTP) deploying two-factor authentication becomes convenient and fast.



- **Strong One-Factor Authentication** – With the unique PortWise Web Keypad, one-factor authentication protects the user and the enterprise from Trojans and Spyware.
- **3rd Party Authentication Support** – PortWise supports up to 14 different methods of authenticating a user including token based solution from RSA, VASCO, and VeriSign making it easy to integrate with your preferred method of authentication, and leverage existing investments.
- **Cost-Effective to Deploy and Manage**– with none of the delivery, breakdown, replacement and on-going management costs of hardware tokens, the PortWise MobileID offers significantly reduced TCO
- **Convenient and Scalable** – requiring no proprietary hardware, the PortWise solution is ideal for large business-to-business or business-to-consumer deployment.
- **Standards-based** – The PortWise MobileID solution supports the latest in open authentication standards (OATH).



SINGLE SIGN-ON & FEDERATED ID's

During a session users typically interact with multiple back-end application and data resources. To simplify the user experience technologies like single-sign on and next generation federated identities mean that disparate application and data resources can appear to the user as one homogenous group.

- **Single Sign-On** – Access to resources without having to repeatedly re-authenticate themselves optimises the user experience. Sign in once to the PortWise Authentication Service, and it does the rest!
- **Identity Federation** – A single digital identity can now be used to access multiple departments or even businesses

without the need for extra and costly user enrolment. Ideal to share identities in business-to-business partnerships, or company/departmental merger scenarios.

- **Standards-based** – By using the latest SAML 2.0 standard, the PortWise solution is compliant with any existing third-party identity federation deployments.



END-POINT INTEGRITY & PROTECTION

Increasingly security attacks are occurring on a user's device (or end-point). With many more end-points now accessing corporate applications and data, checking the integrity of an end-point before allowing access or taking proactive steps to protect it, forms an integral part of providing secure connectivity for users.

- **Deep Device Examination** - Rapid scan of every device (e.g. laptop or PDA) before it connects to the corporate network to match against network, application, file or operating system requirements, e.g. is anti-virus software installed on their end-point, and is it up to date?



- **Real-Time Scanning** - Continuous in-session integrity checking of all connected devices
- **Access Client Security** – Ensures only pre-approved applications can connect to the VPN tunnel, and protects against external connections through the device into the corporate network by making access exclusive
- **Session Cleanup** - Removes all traces of access from the end-point on completion of the session including Cookies, URL History, Cached Pages, Registry Entries and Downloaded Components
- **Third Party End-Point Protection Support** – support for Symantec (Sygate) Secure Desktop
- **Heterogeneous** - ActiveX and Java Support means examination of a broad group of devices



MID-POINT INTEGRITY

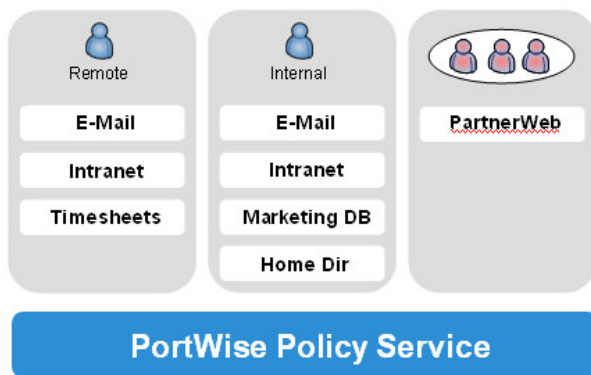
With the advent of evil-twin threats, new measures must be taken to determine the integrity of wireless access points to ensure no leakage of corporate or personal data

- **WPA Authentication** - Authenticate corporate wireless access points with Wi-Fi Protected Access (WPA)
- **Differentiation** – Discriminate between users connecting through a pre-authenticated trusted access point, and an untrusted access point in the IAM policy



IAM POLICY MANAGEMENT

Integrating all aspects of an Identity and Access Management into a single, cohesive and integrated policy delivers significant security, scale and auditing benefits to an organization. Leveraging the five core technologies outlined above, a rich access control policy can be created which adaptively grants the granular application and data resource access based on the security of the users workspace. Factors that can be included in the policy can be:



- **End-Point Integrity** – Grant access based on device type, end-point integrity, etc.
- **Authentication Level** – How did the user authenticate themselves, and how sure are we, that they are who they say they are?
- **User's Role** – Who is the user, and which LDAP groups are they part of? E.g. marketing, sales, engineering, finance, or employee, partner, customer.
- **Network** – Using network information such as MAC Address, or Subnet Mask can help determine how trusted the network is
- **Point of Entry** – Depending on which PortWise Access Point is used (e.g. London, New York, Tokyo) determines which local applications may be seen
- **Mid-Point Integrity** – Grants access based on the security of the Mid-Point Integrity Check



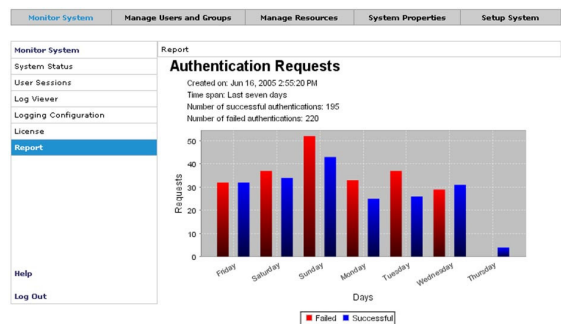
AUDIT

Whether for corporate governance or regulatory compliance with standards such as ISO1771, Sarbanes-Oxley, or Gramm-Leach-Bliley HIPPA, knowing who did what in the enterprise, and which applications were accessed from where is imperative. PortWise includes a number of features to help compliance officers, and corporate governance teams including:

- **Consolidated Audit** – PortWise collects all information about any identity or access activity (user or system-based) in a central repository for easy access. This results in quick

and in-depth insight into the activities across the organization.

- **Comprehensive Audit** – In-depth audit of device assessments, authentication, and access collected in secure central location. Find out exactly who did what, when, where, and how.
- **Graphical Reports** – All information in the PortWise audit logs can be shown in many different graphical formats (pie charts, line charts, 3D charts, bar charts, etc.) in both real-time and over a historical period. Reports can be run in these different categories:
 - Assessments
 - Authentication
 - Authorization
 - VPN Access
 - Audit
 - System Health
 - Performance



- **Exportable Reports** – For further data mining and asset management PortWise can export audit data to Excel or Crystal Reports.



ENTERPRISE ADMINISTRATION

PortWise provides a central administration console for administrating all aspects of identity and access control including end-point integrity, clientless VPN, single sign-on and federated identities, authentication, mid-point integrity, policy management and auditing for reduced administration costs and enterprise scalability. Other features include:

- **Delegated Management** - shift administration rights from one organizational level/department to a lower one
- **Multi-Domain Support** - Domain customisation for User Portal, with central administration
- **Real-Time Alerts** - Threshold based triggers and alerts for proactive awareness through e-Mail and SMS

PortWise

info@portwise.com

For additional information about PortWise, its products, or the location of an office near you, please call our corporate headquarters or visit our Web site at www.portwise.com