

Making Mobile Connections Trusted™

How iPass Policy Orchestration Helps Ensure Enforcement Of Endpoint And Network Security Solutions

- Close gaps in mobile security through coordination of iPass connectivity and best-of-breed security tools
- Protect user identities, mobile endpoint systems, session data, and your corporate network
- Coordinate the use of leading VPNs, personal firewalls, anti-virus packages and patch management systems
- Provide universal enforcement of security and connectivity policies

RECOGNIZING GAPS IN MOBILE SECURITY

Today's remote and mobile workforce poses one of the greatest threats to corporate assets and operations. Security breaches originating from unprotected devices working over the Internet can lead to operational, financial and legal risks - which is why mobile security is a top priority in business today.

Remote and mobile computers "in the wild" are the most difficult to secure. These systems have the highest risk of becoming infected from viruses and other Internet-born threats that take advantage of out-of-date or improperly configured security software. Once end users' computers are compromised, they lose productivity and put their personal and corporate information, the laptops' operation and the enterprise network itself at risk. Remediation is a necessity, but is complicated as remote and mobile devices may only occasionally come back to connect to the corporate network, making "desktop-oriented" remediation systems ineffective.

In an effort to strengthen security for endpoint devices and the corporate network, companies have deployed numerous security point products to address new threats as they arrive. This approach is often a necessity today, however, these point products typically operate in isolation, complicate the user experience and leave dangerous gaps in the enforcement of enterprise security policies. This only exacerbates the threat posed by remote and mobile workers as they connect to the corporate network over the Internet.

TRUSTED MOBILITY – SECURING CONNECTIONS TO HELP PROTECT THE ENTERPRISE

To protect key corporate assets against these connectivity-based threats, iPass has created a unique approach called Policy Orchestration. Through a rich set of capabilities in our core services and deep technology integration, Policy Orchestration enables enterprises to provide ubiquitous connectivity that is easy to use in a controlled, policy-compliant manner. This includes maintaining consistent use of security products across all remote and mobile Internet connections.

Through the Policy Orchestration initiative, iPass is leading an industry evolution from "secure remote access" — basic protection for the authentication process and session data — to "trusted mobility" distinguished by powerful gap-free policy enforcement that protects both endpoints and corporate networks. With services that operate at key points throughout the connection process, iPass is able to integrate, coordinate and enforce policies to close key gaps in protection of endpoints and networks.

Trusted mobility is based on the following core elements:

iPass Corporate Access™ Service: Keeps users connected around the world through ubiquitous dial coverage, mobile data services, in-flight access through Connexion by BoeingSM and over 20,000 Wi-Fi access points, including T-Mobile® HotSpot locations in the U.S.

iPassConnect™ Universal Client: Provides a simple, consistent interface for all connectivity options, on and off the iPass network.



Trusted connections. No compromises.





It also provides a single point of coordination for intelligent enforcement of your security policies across all connection types.

Policy Orchestration Initiative: Focuses on delivering services that close gaps in remote and mobile security through coordination of iPass connectivity services and best-of-breed enterprise security tools.

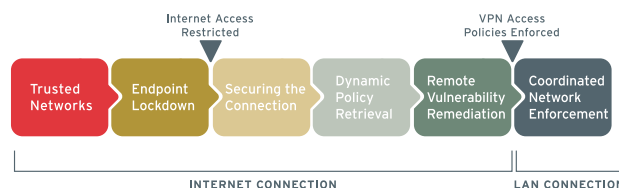
CLOSING THE GAPS THROUGH IPASS POLICY ORCHESTRATION

When security tools operate in isolation from connectivity, gaps in policy enforcement open up. Whether users connect by DSL without personal firewall protection or get access to unsecured Wi-Fi networks, they become targets for worms, viruses or worse because they missed critical security patches.

iPass Policy Orchestration closes these critical security gaps by tightly linking security and connectivity. It does this through deep technical integration of the iPassConnect client with an array of security services. By coordinating leading authentication, authorization and patch management tools, Policy Orchestration brings better protection for user identities, mobile and remote systems and the enterprise network.

This first-of-its-kind, vendor-agnostic approach allows IT staff to enforce security policy compliance for Internet and VPN use over all connections - even over non-iPass networks. Only users and devices that first conform to endpoint security policies receive access. If a user's security software is not running or is out of date, remediation is initiated on-the-fly or their connection is blocked.

Policy Orchestration achieves all this through a secure connection process that helps keep IT in control, while keeping users secure and productive. The process is made up of functionality that spans six key categories that can be implemented completely for maximum benefit, or in stages.



How Policy Orchestration Works. The endpoint is locked down whenever the user attempts an Internet connection and VPN access is only allowed after successful completion of a series of policy checkpoints, including on-the-fly endpoint remediation. Finally, network protection can be enforced in conjunction with leading network enforcement solutions.

TRUSTED NETWORKS

The iPass global virtual network delivers an added layer of network trust. Every network provider is certified enterprise-ready and has been tested for connection quality and enterprise systems compatibility.

On the iPass network, authentication is protected by these additional measures:

iPass Secure End-to-End Encrypted Login (iSEEL): Advanced public-key cryptography is used to protect passwords against eavesdropping and replay attacks. User passwords remain encrypted with iSEEL for safe transmission across access-provider networks and the Internet.

Digital Certificate Exchange: Mutual digital certificate exchanges are performed at every point in the authentication process over the iPass network of enterprise-ready providers. This verifies the identity of the systems communicating with one another during any transaction, to prevent rogue devices from entering the authentication loop.

SSL-Protected Authentication: 128-bit SSL tunnels are used across each and every step of the iPass authentication process to ensure that credentials are not stolen or used in a replay attack to gain unauthorized access.

Policy Orchestration capabilities are also supported over non-iPass networks for customers who want to allow more open use of their own network or public networks. This ensures that endpoints and networks are protected directly, while leaving authentication security to the network provider.

LOCKDOWN OF THE ENDPOINT ENVIRONMENT

iPass provides the unique ability to lock down the endpoint and restrict it from communicating over the Internet while in an un-verified and un-trusted state. This helps protect the endpoint from infection by Internet-based threats during the process of user authentication and endpoint remediation.

Endpoint Self-Quarantine: iPassConnect applies different firewall rules based on the connectivity state. This approach restricts endpoint device access to iPassConnect communications with iPass servers as part of the policy enforcement, re-opening the firewall after compliance is confirmed. This protects the endpoint from attack during the policy enforcement process and also can restrict Internet access for devices that fail these compliance checks.

DeviceID: This unique service establishes the trustworthiness of endpoint devices by confirming device properties, issuing a one-time password and linking both to VPN authentication. By adding device-based authentication, you can link user identity to corporate-approved devices and requirements for specific endpoint security software. You gain the flexibility to apply

tighter access controls and enforce compliance with endpoint security policies before granting VPN access.

Endpoint Self-Quarantine*: The iPassConnect client applies different firewall rules based on the device's connectivity state. This approach only allows the endpoint to communicate with specific iPass policy enforcement servers. Once compliance is confirmed, the firewall is re-opened to allow other communication. This protects the endpoint from attack during the policy enforcement process and also can restrict Internet access for devices that fail these compliance checks.

DeviceID™ Service: This unique service establishes the trustworthiness of endpoint devices by confirming device properties, issuing a one-time password and linking both to VPN authentication. By adding device-based authentication, you can link user identity to corporate-approved devices and requirements for specific endpoint security software. You gain the flexibility to apply tighter access controls and require successful completion of vulnerability remediation before granting VPN access.

SECURING THE CONNECTION

Creating and maintaining secure connections requires several interdependent technologies and processes. The iPassConnect client seamlessly coordinates the interaction of personal firewall, anti-virus and VPN technologies without requiring any intervention by users or IT staff.

SecureConnect: iPassConnect automatically invokes personal firewall, anti-virus and VPN products for the user to ensure the endpoint is protected before Internet authentication. When used in coordination with DeviceID, VPN launch can be conditional, based on the operation of other security tools.

Auto-Teardown: This capability complements SecureConnect by terminating the Internet session if any security product stops running for any reason, ensuring the remote device is always protected.

DYNAMIC POLICY RETRIEVAL

The IT administrator has the ability to implement and change access control and security policies from a central location. Once the user is authenticated and successfully connected to the Internet, these policies are automatically applied to the device through the iPassConnect client. These updates can be defined by location, access type, user group or individual so you can restrict access in certain countries or disallow specific users from different access modalities.

Security settings can be applied remotely across any supported security products and access methods, without physically touching the endpoint device or disturbing the end-user experience. Changes can be made anytime and automatically pushed out to end users whenever they connect to the Internet.

REMOTE VULNERABILITY ASSESSMENT AND REMEDIATION

Since simply blocking non-compliant users would hurt workforce productivity, there must be a mechanism for taking corrective action when detecting a policy violation.

Endpoint Policy Management™ Service: This service from iPass automates vulnerability remediation and patching of mobile systems over any Internet connection. Following dynamic policy retrieval, Endpoint Policy Management is invoked by the iPassConnect client and measures the device against current security policies stored on a central server. Endpoint Policy Management downloads and installs the appropriate security patches and anti-virus definition files to bring the device into compliance. Endpoint Policy Management complements standard software distribution products, so that even devices that infrequently contact the corporate LAN are kept up to date.

KEY BENEFITS OF POLICY ORCHESTRATION

True Enforcement Through Coordination: Gain control over VPN access to your network by using the iPassConnect universal client. Rest assured that connectivity and security policies are enforced so only compliant devices get connected.

Built-in Assessment and Remediation: Update endpoint software on the fly over the Internet to ensure devices are protected whenever they connect and users are not needlessly blocked from access.

Optimized for Mobile Productivity: Provide mobile and remote users with a secure connectivity solution that helps them stay productive by making it easy to stay policy compliant.

Works Over Any Internet Connection: Ensure VPN policy enforcement and gain a deep level of policy-based access control when users connect over the iPass global virtual network and non-iPass networks.

Convenient and Centralized Control: Apply access control policies easily from a central point of control via the iPass Portal.

Flexible, Open Architecture: Leverage your investments through robust integration of iPass services with the best-of-breed security products that best meet your needs.



Universal Policy Enforcement: Combine the capabilities of three iPass offerings to provide universal enforcement of security and connectivity policies. Ensure that users go through policy checkpoints by forcing the use of iPassConnect for Internet access, restricting VPN use through DeviceID and requiring assessment and remediation through Endpoint Policy Management. With all three in place, you can make VPN launch conditional, based on remediation and device authentication. A one-time password is issued by DeviceID allowing iPassConnect to launch a VPN connection only if the endpoint passes all policy check points, undergoes necessary corrective action and is deemed compliant. In this way, you can restrict access to devices that are protected and ensure that remote and mobile workers get the security updates they need to obtain full network access and stay productive.

COORDINATED NETWORK ENFORCEMENT

While iPass services protect the corporate network from users coming in over the VPN, your network is also vulnerable to devices attempting to connect over the LAN. That's why iPass integrates with leading network enforcement products. By integrating network enforcement capabilities into iPass Policy Orchestration, iPass can provide enterprise IT departments with data to make better decisions about the devices that are attempting to connect to your network. Having this

information available makes for a more powerful solution than any collection of point products. Similarly, Policy Orchestration can provide information to third-party patch management systems that assess and remediate network machines for compliance with application updates. Whatever systems you have in place, iPass can make them work smarter for you.

MORE CONTROL, LESS COMPROMISE

The iPass Policy Orchestration initiative and supporting technologies take remote and mobile access to the next level, providing additional security services that ensure more protected endpoint devices and contribute to a more secure network overall. Getting remote and mobile users onto the corporate network has its share of challenges, and a lot of care is required to secure that process. But now there's a solution to greatly simplify this process. The iPass Policy Orchestration initiative puts you in control of remote and mobile endpoints connecting to your network — and enables you to keep them secure without compromising workforce productivity and IT staff efficiency.

Learn more at www.ipass.com today. ■

EXTENDING ENTERPRISE SECURITY

iPass services are integrated with products from these leading vendors. A products listing can be found at www.ipass.com.

VIRTUAL PRIVATE NETWORKS

- Aventail
- Check Point
- Cisco Systems
- Juniper
- Microsoft
- NCP
- Nortel Networks

PERSONAL FIREWALLS AND INTRUSION DETECTION SYSTEMS

- Check Point (Zone Labs)
- Internet Security Systems
- Sygate

ANTI-VIRUS SOFTWARE

- Computer Associates
- McAfee
- Symantec
- Trend Micro

AAA

- Active Directory
- RADIUS
- LDAP

NETWORK ENFORCEMENT PRODUCTS

iPass interoperates with products from:

- Check Point (Zone Labs)
- ENDFORCE
- InfoExpress

- Nortel
- Senforce
- Sygate

INDUSTRY ORGANIZATIONS

iPass is a member of:

- Cisco Network Access Control
- Microsoft Network Access Protocol
- TCG Trusted Network Connect

* Self-Quarantine functionality is possible through integration with Sygate products.

Corporate Headquarters
iPass Inc.
3800 Bridge Parkway
Redwood Shores, CA 94065

+1 650-232-4100
+1 650-232-4111 fx

www.ipass.com

