

iPass[®] Encrypted Login

Protect User Passwords From The Client Device To The Enterprise

- A software-based one-time password solution
- Protect against credential theft over dial-up, wireless and shared wired broadband links
- Encrypt authentication credentials within 128-bit SSL tunnels until they are inside the enterprise network
- Boost security without extra steps for the user



There's a reason people put locks on doors, alarms on cars and authentication challenges on networks. It's equally important to protect the keys that fit those locks, the remotes that disable those alarms and the passwords that meet those authentication challenges. That's why iPass incorporated Encrypted Login technology into our network architecture and universal client to protect user authentication credentials.

Encrypted Login is a valuable component of the iPass[®] Mobile Office service that provides an additional layer of password protection. This unique technology protects passwords from the client device all the way to the enterprise by combining public-key cryptography and unidirectional SSL tunneling to encrypt passwords traveling over risky "first mile" connections and the public Internet.

PREVENT CREDENTIAL THEFT OVER BROADBAND LINKS

Encrypted Login technology begins on the client device. The iPassConnect[™] universal client uses a public key and 131-bit elliptical-curve cryptography to create an encrypted one-time ASCII password based on username, a unique service interface ID and a session counter.

This technology protects against credential theft over dial-up, wireless and shared wired broadband links. Even if the one-time password is sniffed, it's useless to a would-be attacker since it can't be decrypted without the private key stored at the iPass Transaction Center. And any attacks based on reusing the encrypted password will be mitigated since the password changes with each user session.

PROTECT TRANSMISSIONS ALL THE WAY TO YOUR NETWORK – NO SHARED SECRETS

Once authentication requests are within the iPass network — starting from the iPass NetServer[™] at the access provider's site — iPass encrypts them within 128-bit SSL tunnels until they are inside the enterprise network. All SSL tunnels are unidirectional and based on a valid digital signature from the sender, ensuring that iPass systems only talk with other authorized iPass systems.

Because user authentication credentials aren't decrypted until they are safely within the iPass Transaction Center, network access providers never have access to clear-text passwords. In addition, access providers never have access to enterprise IP addresses, port addresses or private authentication keys. This provides an additional layer of protection in the event that there's loose security or a malicious employee at an access provider.

HOW ENCRYPTED LOGIN WORKS

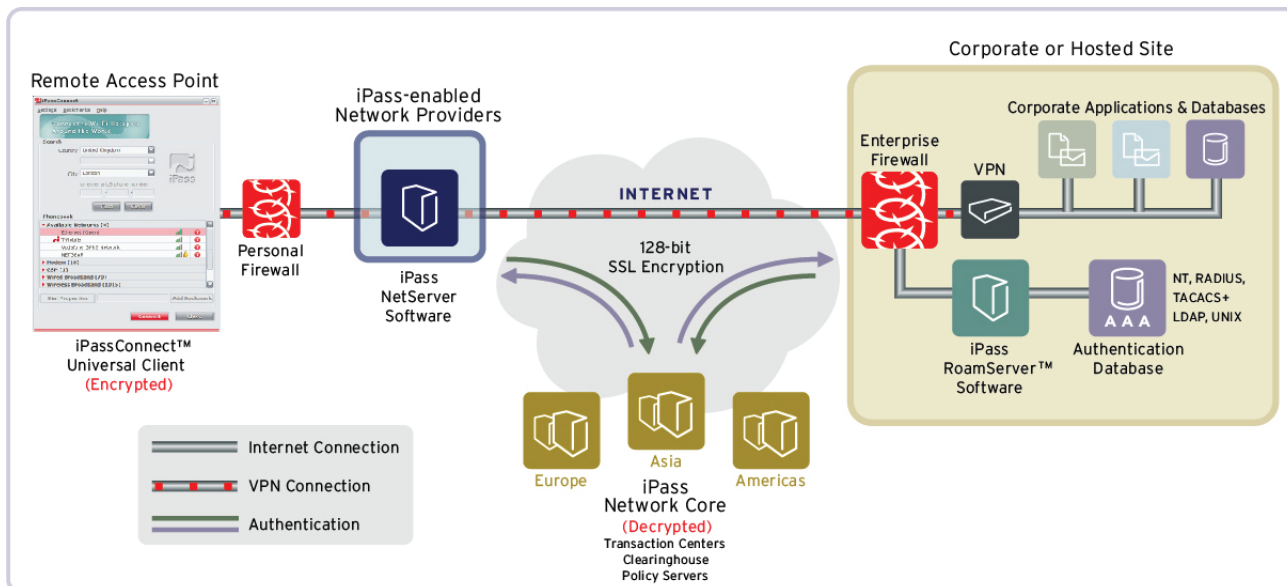
1. Encrypted Login runs on iPassConnect and uses a public key to create an encrypted one-time password based on username, a unique service interface ID and a session counter.
2. iPassConnect then sends the encrypted password via a wireless or wired broadband link to the iPass NetServer at the access provider's site.
3. The iPass NetServer creates an SSL tunnel to an iPass Transaction Server at the nearest regional iPass Transaction Center, which uses the enterprise's private key to decrypt the password – the access provider never has access to the decrypted credentials. The iPass Transaction Center then routes the password on to the company's hosted iPass RoamServer[™] via another SSL-protected tunnel.



4. The iPass RoamServer checks the decrypted password against the enterprise's local authentication server, which either allows or denies access.
5. The iPass RoamServer forwards the response back to the iPass NetServer via the Transaction Center.
6. If the response is positive, the iPassConnect client launches the VPN to establish a secure, direct tunnel between the user's device and corporate network resources, including e-mail and Internet access.

BOOST NETWORK SECURITY TODAY

Encrypted Login increases your enterprise's network security by protecting user credentials from end to end. Its multi-layered approach to security offers virtually unbeatable protection across a global virtual network — to ensure that what's yours stays yours. The best part is that this valuable technology is built into all the components of the iPass network and comes standard as part of the iPass Mobile Office service. For more information, visit www.ipass.com or talk to your iPass account manager today. ■



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

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

www.ipass.com

