HyTrust two-factor authentication for VMware

Strong security and compliance for vSphere and NSX virtual infrastructure

- Privileged IT admin accounts require strong protection from cyber attackers if sensitive data is to be protected
- Two-factor authentication is mandatory for privileged accounts because it prevents an unauthorized person from using the account to steal data or compromise IT infrastructure
- Two-factor authentication on IT administration accounts is commonly required by compliance regimens such as PCI DSS 3.0 or NIST 800-53
- Two-factor authentication should be used in conjunction with role-based authorizations (RBAC) for even more stringent controls and separation of duties.

The privileged administrator account risk

Privileged accounts are frequent targets of cyber criminals and therefore must be well protected. These accounts are normally used by IT administrators to configure and maintain a wide variety of hardware and software assets, including applications, databases, and virtual infrastructure. Privileged accounts often have broad access to sensitive data and can bypass normal access control restrictions. These accounts can even be abused to disable or delete activity logging, allowing a malicious insider or external attacker to "cover their virtual tracks" and remain undetected. This is why privileged accounts are such ripe targets for attackers, and why compliance regimens such as PCI, NIST or HIPAA always include control objectives on these accounts.

Securing infrastructure with two-factor authentication

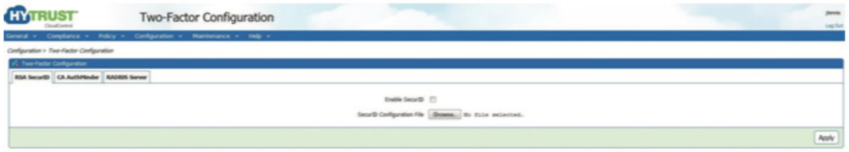
The most important and fundamental control to protect privileged accounts is "strong authentication". Authentication is the process of validating that a login request is originated by someone who is indeed "authorized" to use the account. The most familiar authentication method is a simple username and password combination. This may be adequate for a personal email account, but it most definitely is not sufficient for a privileged IT account. Passwords can be guessed, or obtained via session hijacking attacks and keyloggers on client PCs. They can also be shared improperly, as happened when Edward Snowden's colleagues gave him their admin account passwords and he used them to collect confidential documents by the thousands.

Strong authentication simply refers to an authentication method that is more robust than a simple username/password, making it harder to misuse the account. Usually strong authentication is implemented using "two-factor authentication", which means that two different things are required to successfully log in. This might be a combination of something you know (a password), with something you have (your fingerprint or a hardware token). *The key advantage of two factor authentication is that simply borrowing or stealing the password will not be enough to gain access to a privileged account.*

Unfortunately many critical IT systems (for example VMware vCenter) do not include two factor authentication. They support a simple local database of usernames and passwords, or Active Directory (AD) integration. A common misconception is that AD integration provides two factor authentication, however this is not the case. Active Directory integration allows a system to use the centralized usernames, passwords, and account policies in AD, rather than having to manage these objects on the system itself. While very valuable, this integration does not provide two-factor authentication: a username/password can be misused just as easily with AD integration as without it.

HyTrust CloudControl™ – two-factor authentication for VMware

To meet security and compliance requirements for their virtualized data centers and private clouds, enterprises rely on HyTrust. HyTrust CloudControl provides the broadest range of controls for VMware system administration available. This control set includes two factor authentication using RSA SecurID, CA, RADIUS and smartcards. (Support for NSX virtual networking and TACACS+ has also been announced and will be available in early 2015.) HyTrust CloudControl is required for two-factor authentication on vCenter, vSphere and NSX because none of these products support two-factor on their own. VMware has partnered with HyTrust to deliver two factor authentication, and has invested in the company because of the important security features that HyTrust brings to VMware environments.



Enable SecurID □

SecurID Configuration File No file selected.

HyTrust CloudControl supports a broad range of two-factor authentication options for privileged administrators.

Beyond two-factor authentication — role-based access controls

For additional security, HyTrust CloudControl augments two-factor authentication with both role-based and label-based authorization (RBAC) controls on VMware admin accounts. RBAC allows organizations to define policy that controls, monitors and alerts on administrative actions. CloudControl RBAC supports restricting an admin account to only perform certain operations, or only operate on certain objects. For example, a "PCI admin" could be authorized to work with the virtual servers within the PCI cardholder data environment, but nothing else. Or a junior IT operator could be prohibited from performing potential risky actions like shutting down a production virtual server without approval from a more senior employee.

Role-based authorizations go well beyond strong authentication to support segregation of duties and risk mitigation for critical virtual infrastructure. By combining CloudControl's two-factor authentication, role based access controls and robust logging, organizations can implement an effective barrier to cyber attacks and meet compliance requirements in an operationally efficient manner.

Function	**HyTrust CloudControl**
Two-factor authentication	●
Role-based authorizations	●
Forensics quality logging of admin actions	●
vSphere configurations hardening	●

HyTrust CloudControl provides the industry's most complete control set for virtual infrastructure administration.

Learn more about HyTrust at www.hytrust.com or call us at 844-681-8100.

HyTrust - Cloud Under Control.
1975 W. El Camino Real, Suite 203
Mountain View, CA 94040, USA
Phone: 1-844-681-8100
International: 1-650-681-8100