



# Implementing Secondary Approval, or the “Two-Person Rule”



## INTRODUCTION

# Executive Overview

Enterprises increasingly seek to virtualize their mission-critical workloads in order to achieve financial objectives. At the same time, they are realizing they must monitor and control VMware privileged administrator access to virtual machines (VMs) in order to ensure the security and regulatory compliance of their Tier 1 applications. They also want to maintain virtualization operations productivity, so access controls must have the flexibility to fit the way the virtualization team works day to day.

The Secondary Approval automated workflow provided by Entrust CloudControl overcomes the challenge of efficiently securing access to critical VMs. By enforcing the “two-person rule” for high-impact administrative operations, Secondary Approval prevents costly disruptions caused accidentally or intentionally by a VMware privileged administrator. The flexible, situation-specific access control enabled by Secondary Approval helps keep virtual data centers productive, secure, and compliant with regulations.

**Entrust has become the de facto standard for access control, logging, and policy enforcement in VMware environments.**

## The Challenge

Privileged administrators of the VMware vSphere platform typically have much greater administrative power than their counterparts who manage physical data center infrastructure. They can copy, power off, or delete a virtual machine that hosts a production application – accidentally or intentionally – with a few clicks. If the result is substantial operations downtime, a serious compliance violation, or a confidential data breach, the cost can be dramatic. Recent high-profile breaches in which vSphere admins destroyed production data center resources through the management interface demonstrate that the risks are real.

Entrust access control policies based on “always on” rules provide very effective protection for critical applications and data in VMs. At the same time, data centers often want an efficient way to grant VMware admins temporary administrative privileges needed to perform infrequent job duties. In other situations, managers want greater control over the use of powerful privileges by admins who need those privileges to do their jobs every day.

### Examples of these situations include:

- A contractor occasionally clones the VM that hosts the enterprise email server in order to test patches and upgrades. The enterprise wants to ensure that the contractor cannot clone the VM for any other reason.
- A group of vSphere admins conducts monthly scheduled reboots of VMs that run production workloads. Management wants to enable the reboots each month without having to approve exceptions, but also wants to require one-time approval for all other VM power-off and power-on operations.
- A virtualization operations group needs ongoing authorization to create and delete VMs used for non-production applications. However, their manager wants the ability to approve or deny any attempt to delete a production VM.

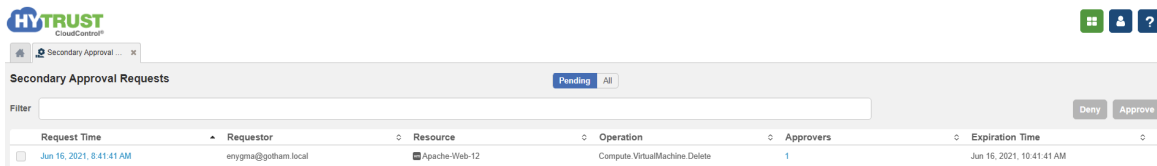
The VMware platform does not provide a viable way to enable one-time authorization of a particular operation attempted by a particular user. Consequently, many enterprises have been hesitant to virtualize their critical workloads and have missed the economic gains available from greater virtualization.

## The Entrust Solution

Entrust makes secure multi-tenancy possible by closing gaps in virtual infrastructure. An administrator can clone a VM holding another tenant's sensitive data, for instance, knowing that the action can't be traced back to them. Enterprise cloud owners and Cloud Solution Providers (CSPs) must be able to monitor and record each vSphere admin's activity at all times in order to ensure accountability and prove compliance with regulations. Traditional firewalls do not mitigate these visibility and control risks.

Secondary Approval workflow increases the power and flexibility of Entrust CloudControl by enforcing the "two-person rule". According to US Air Force Instruction (AFI) 91-104, the two- person rule is designed to prevent accidental or malicious launch of nuclear weapons by a single individual. Similarly, the automated Secondary Approval process requires a designated approver to authorize an administrative operation attempted by a privileged user before the operation can proceed.

The Secondary Approval workflow is simple and efficient, making it easy for operations groups to implement. It begins when a user attempts a VMware platform operation requiring authorization, in accordance with data center policy. Entrust CloudControl blocks execution and tells the user that Secondary Approval has been requested for the operation. Entrust CloudControl simultaneously alerts an approver group that a user request requires review, and it provides the details of the request. When an approver makes a decision, Entrust CloudControl notifies the user and – if the request is approved – gives the user an approver-defined window of time in which to execute the approved operation.



Request Time	Requestor	Resource	Operation	Approvers	Expiration Time
Jun 16, 2021, 8:41:41 AM	ernygn@gotham.local	Apache-Web-12	Compute.VirtualMachine.Delete	1	Jun 16, 2021, 10:41:41 AM

## SUMMARY

By deploying Entrust CloudControl with Secondary Approval, IT organizations take an essential step toward virtualizing their critical workloads and increasing their virtualization ROI without sacrificing security, compliance, or productivity.

For more information on how Entrust enables greater virtualization of workloads that must stay compliant, visit <https://www.entrust.com/products/cloudcontrol/>, email questions to [sales@entrust.com](mailto:sales@entrust.com), or call Entrust at 650-681-8100 for a free consultation.

**Secondary Approval workflow increases the power and flexibility of Entrust CloudControl by enforcing the “two-person rule”. According to US Air Force Instruction (AFI) 91-104, the two-person rule is designed to prevent accidental or malicious launch of nuclear weapons by a single individual.**

For more information

**888 690 2424**

**+1 952 933 1223**

**sales@entrust.com**

**entrust.com**

## ABOUT ENTRUST CORPORATION

Entrust is dedicated to securing a world in motion by enabling trusted identities, payments, and data protection. Today more than ever, people demand seamless, secure experiences, whether they're crossing borders, making a purchase, accessing e-government services, or logging into corporate networks. Entrust offers an unmatched breadth of digital security and credential issuance solutions at the very heart of all these interactions. With more than 2,500 colleagues, a network of global partners, and customers in over 150 countries, it's no wonder the world's most entrusted organizations trust us.

Learn more at  
**entrust.com**



Entrust and the Hexagon logo are trademarks, registered trademarks, and/or service marks of Entrust Corporation in the U.S. and/or other countries. All other brand or product names are the property of their respective owners. Because we are continuously improving our products and services, Entrust Corporation reserves the right to change specifications without prior notice. Entrust is an equal opportunity employer.  
© 2021 Entrust Corporation. All rights reserved. HS22Q1-dps-secondary-approval-sb

Global Headquarters  
1187 Park Place, Minneapolis, MN 55379  
U.S. Toll-Free Phone: 888 690 2424  
International Phone: +1 952 933 1223  
**info@entrust.com** [entrust.com/contact](https://entrust.com/contact)