



# VMware vSphere and Entrust CloudControl

Integration Guide

2024-12-20

© 2025 Entrust Corporation. All rights reserved.

# Table of Contents

1. Introduction	1
1.1. Product configurations	1
1.2. Requirements	1
2. Procedures	2
2.1. Download the CloudControl software	2
2.2. Deploy the CloudControl VM from the OVA	2
2.3. Power on the appliance	3
2.4. Configure the CloudControl virtual appliance	3
2.5. Set up the CloudControl GUI	3
2.6. Add vCenters to CloudControl	4
2.7. Enable Global PIP	8
2.8. Add local users to the system	10
2.9. Test the vCenter Published IP (PIP) and ESXi Hosts Global IP (GPIP) addres	S
	10
and ports	10
and ports	
and ports 2.10. Configure email 2.11. View the vSphere inventory	
and ports 2.10. Configure email 2.11. View the vSphere inventory 2.12. Logs	10 11 12 12
and ports 2.10. Configure email 2.11. View the vSphere inventory 2.12. Logs 2.13. Access Control.	10 11 12 12 13
and ports 2.10. Configure email 2.11. View the vSphere inventory 2.12. Logs 2.13. Access Control 2.14. Secondary Approval	10 11 12 12 13 17
<ul> <li>and ports.</li> <li>2.10. Configure email</li> <li>2.11. View the vSphere inventory.</li> <li>2.12. Logs.</li> <li>2.13. Access Control.</li> <li>2.14. Secondary Approval.</li> <li>2.15. Configuration Hardening.</li> </ul>	10 11 12 12 13 17 20
<ul> <li>and ports.</li> <li>2.10. Configure email</li> <li>2.11. View the vSphere inventory.</li> <li>2.12. Logs.</li> <li>2.13. Access Control.</li> <li>2.14. Secondary Approval.</li> <li>2.15. Configuration Hardening.</li> <li>2.16. Remediation Policy</li> </ul>	10 
<ul> <li>and ports.</li> <li>2.10. Configure email</li> <li>2.11. View the vSphere inventory.</li> <li>2.12. Logs.</li> <li>2.13. Access Control.</li> <li>2.14. Secondary Approval.</li> <li>2.15. Configuration Hardening.</li> <li>2.16. Remediation Policy</li> <li>3. Troubleshooting.</li> </ul>	10 
<ul> <li>and ports.</li> <li>2.10. Configure email</li> <li>2.11. View the vSphere inventory.</li> <li>2.12. Logs.</li> <li>2.13. Access Control.</li> <li>2.14. Secondary Approval.</li> <li>2.15. Configuration Hardening.</li> <li>2.16. Remediation Policy</li> <li>3. Troubleshooting.</li> <li>3.1. Host Credentials: Certificate Invalid.</li> </ul>	10 
<ul> <li>and ports</li> <li>2.10. Configure email</li> <li>2.11. View the vSphere inventory.</li> <li>2.12. Logs</li> <li>2.13. Access Control.</li> <li>2.14. Secondary Approval.</li> <li>2.15. Configuration Hardening.</li> <li>2.16. Remediation Policy</li> <li>3. Troubleshooting</li> <li>3.1. Host Credentials: Certificate Invalid.</li> <li>4. Additional resources and related products.</li> </ul>	10 
and ports. 2.10. Configure email 2.11. View the vSphere inventory. 2.12. Logs 2.13. Access Control. 2.14. Secondary Approval. 2.15. Configuration Hardening. 2.16. Remediation Policy 3. Troubleshooting 3.1. Host Credentials: Certificate Invalid. 4. Additional resources and related products. 4.1. CloudControl.	10 
<ul> <li>and ports.</li> <li>2.10. Configure email</li> <li>2.11. View the vSphere inventory.</li> <li>2.12. Logs</li> <li>2.13. Access Control.</li> <li>2.14. Secondary Approval.</li> <li>2.15. Configuration Hardening.</li> <li>2.16. Remediation Policy</li> <li>3. Troubleshooting.</li> <li>3.1. Host Credentials: Certificate Invalid.</li> <li>4. Additional resources and related products.</li> <li>4.1. CloudControl</li> <li>4.2. Entrust products</li> </ul>	10 11 12 13 17 20 

# Chapter 1. Introduction

Entrust CloudControl integrates with VMware vSphere by protecting your vCenters and ESXi hosts. CloudControl organizes your vSphere inventory into categories to help you find information about your vSphere deployment. With vSphere, you must keep insiders such as virtual administrators in their "swim lanes." CloudControl uses role and asset-based access control to help you define who can do what to which objects. It also uses workflows supporting secondary approval for sensitive and high impact operations. Entrust CloudControl identifies configuration errors in VMware vSphere hosts using pre-built assessment frameworks. It uses active remediation and proactive monitoring ensuring ongoing compliance.

# 1.1. Product configurations

Entrust has successfully tested the integration of Entrust CloudControl with VMware vSphere in the following configurations:

System	Version
VMware vSphere	7.0.3 and 8.0.0
Entrust CloudControl	6.6.0

# 1.2. Requirements

Before starting the integration process, familiarize yourself with:

- The documentation and setup process for VMware vSphere.
- The documentation and setup process for Entrust CloudControl. The online documentation contains everything needed to successfully install and deploy CloudControl.



Entrust recommends that you allow only unprivileged connections unless you are performing administrative tasks.

# Chapter 2. Procedures

It is important to note that this guide uses a standalone CloudControl deployment and does not use Active Directory. Users are local to the system. CloudControl was not configured to use Active Directory. CloudControl also supports a cluster environment and this will be documented in the installation guide.

# 2.1. Download the CloudControl software

- 1. Go to https://my.hytrust.com/s/software-downloads.
- 2. Log in and select HyTrust CloudControl.
- 3. Open the folder HTCC\_6.6.0\_2023-02-24. This folder contains version 6.6.0 that was used in this guide.
- 4. Select the Entrust-CloudControl-6.6.0.660934.zip link to download the file.

Case	es Knowledge Base 🗸 Product Documentation	Licenses	Software Downloads	Upgrade Center	Videos	
So	fware Downloads					
♥ Hytri	ust CloudControl					
	Folder Name					
	HTCC_MoveRPVTool_2020-10-15					
	HTCC_Migration_Tool_2021-05-19					
	HTCC_6.6.0_2023-02-24					
	Action Name					Size
	Entrust_CloudControl_Release_Notes_v6.6.pdf	_				0.19 MB
	Entrust-CloudControl-6.6.0.660934.zip					6399.99 MB
~	Entrust-CloudControl-6.6.0.660934.zip.sha256sum.txt					104 Bytes
0	Entrust-CloudControl-6.6.0.660934.zip.sha384sum.txt					136 Bytes
	Entrust-CloudControl-6.6.0.660934_upgrade.zip					3788.62 MB
	Entrust-CloudControl-6.6.0.660934_upgrade.zip.sha256	sum.txt				112 Bytes

5. Once the file has been downloaded, open the ZIP file to access to the OVA file.

# 2.2. Deploy the CloudControl VM from the OVA

- 1. Log in to vCenter.
- 2. Navigate to Inventories > Hosts and Clusters.
- 3. Select the resource pool where you plan to deploy CloudControl.
- 4. Select Actions > Deploy OVF Template from vSphere Web Client.



5. On the Select an OVF Template page, select **Local File** and upload the Entrust-CloudControl-6.6.0-660934.ova file.

Deploy OVF Template	Select an OVF template Select an OVF template from remote URL or local file system	×
Select an OVF template     Select a name and folder	▲ If you use the vSphere Client to deploy an OVF template with a virtual TPM device, the device is not deployed. You can add the device to the destination VM after the deployment completes. Alternatively, use the ovftool to deploy OVF templates with TPM devices.	
3 Select a compute resource	Enter a URL to download and install the OVF package from the Internet, or browse to a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.	
4 Review details		- 1
5 Select storage	Local file	- 1
6 Ready to complete	UPLOAD FILES Entrust-CloudControl-6.6.0-660934.ova	
	CANCEL	т

Follow the instructions on Deploying CloudControl as required.



For more information refer to Installing CloudControl from an OVA in the online documentation.

# 2.3. Power on the appliance

- 1. Log in to the vSphere Client.
- 2. Locate the Entrust CloudControl virtual machine in the inventory.
- 3. Right-click the CloudControl virtual machine and select **Power > Power On**.

# 2.4. Configure the CloudControl virtual appliance

This guide uses a Standalone Node setup. Follow the online documentation for instructions for Creating a Standalone Node.

# 2.5. Set up the CloudControl GUI

Once the standalone node has been configured, you must finish the setup using the GUI. Follow the online documentation instructions on Setting Up the CloudControl GUI.

# 2.6. Add vCenters to CloudControl

You can now add the VMware vSphere inventory into CloudControl.

#### 2.6.1. Add a vCenter to CloudControl

To add a vCenter to CloudControl:

- 1. From the Home tab, select **Inventory > vSphere**.
- 2. On the vSphere page, select **Actions > Add vCenter**.

Add vCenter @ 10.194.	
1: About – 2: Configure – 3: Details – 4: Onboard Hosts – 5: Host Credentials	
IP/FQDN *	
10.194.	Adding vCenter
Port*	All linked vCenters will be discovered starting from the IP/FQDN provided.
443	Service Account
Service Account     Managed Credentials Account	The vCenter service account to be used for CloudControl. The same account must be used across all vCenter Servers, and it must have administrator privileges.
Service Account*	Managed Condentials Associat
administrator@	Access service account credentials from a
Service Account Password *	stored credential management account. View or add an account in credentials
	management.
Continue	

#### 2.6.2. Configure CloudControl after adding a vCenter

To configure CloudControl after adding a vCenter:

- 1. On the **Configure page**, view and approve the certificates for the Platform Services Controller (PSC) and all vCenters that were discovered.
- 2. The **Approve** checkbox must be checked for all certificates before you can add the vCenter.
- 3. Certificates from a trusted source have the Approve checkbox checked automatically.
- 4. Select the **Certificate** link to view the certificate details.

Certificates without a certificate authority are displayed with a warning icon. Select the link in the tool tip to add a CA. You can manually approve these certificates by checking the **Approve** checkbox. Certificates that are invalid or expired are displayed with an error icon. These certificates cannot be approved. All vCenter and PSC certificates are displayed on the **Certificate Authorities** tab on the **Certificates** page.

- 5. Select **Approve** to populate the approve checkbox for the certificate, or select the **x icon** to close the window.
- 6. Determine if you want to use a single Published IP for each vCenter or a Published IP Range to be used for all current and future vCenters in this ELM.

If you plan to use Access Control, you must have a Published IP address or range.

- 7. For a Published IP, select the **Configure** link in the **Published IP** column of the vCenter table, enter the Published IP Address and Netmask, and select **Apply**.
- 8. For a Published IP Range, enter the **Published IP Address** and **Netmask** in the **Published IP Range** section.
- 9. Enable **Tag Sync** if you want vCenter Tags in CloudControl.

🐇 🕛 System Settings 🗙 🛃 vSphere 🗙 🕇 Add vCenter	×	
Add vCenter @ 10.194.		
1: About 🗸 - 2: Configure - 3: Details - 4: Onboard Hosts - 5: Host Credentials		
		Approve Certificates
The following PSCs and vCenters were discovered		Each PSC and vCenter discovered needs an approved certificate in order to be added to
Platform Services Controller		CloudControl.
Name	Certificate	Configure Published IP
10.194.	Approve (View)	Configuring a Published IP for each vCenter will help protect access to the vCenter by routing all requests via ClaudControl
vCenters		
Approve certificates and, optionally, configure an individual Published IP or IP range for access	control protection for each vCenter.	Provide a Published IP address for each vCenter or
		use the IP Range.
vCenter Published IP	Certificate	use the IP Range. Setting up a Published IP for the vCenter is optional
vCenter Published IP 10.194. Configure	Certificate Approve (View)	use the IP Range. Setting up a Published IP for the vCenter is optional but is required for Access Control. Published IP access can be set up after the onboarding process
VCenter Published IP 10.194 Configure Published IP Range	Certificate	use the IP-Kange. Setting up a Published IP for the vCenter is optional but is required for Access Control. Published IP access can be set up after the onboarding process as well.
VCenter         Published IP           10.194         Configure           Published IP Range         If you want to use a Published IP Range instead of providing an individual Published IP for each	Certificate Certificate Approve (View) vCenter, enter the IP range and netmask here.	use the ter karner. Setting up a Published IP for the vCenter is optional but is required for Access Control. Published IP access can be set up after the onboarding process as well. Published IP Range Abriefender IB Pages can be used to reactify a
VCenter         Published IP           10.194         Configure           Published IP Range         If you want to use a Published IP Range instead of providing an individual Published IP for each IP Range	Certificate Certificate Approve (View) vCenter, enter the IP range and netmask here.	use the similar Hange. Setting up a Vublished IP for the vCenter is optional but is required for Access Control. Published IP access can be sit up after the enboarding process as well. Published IP Range A Published IP Range can be used to specify a range of Published IP Range can be used for all
VCenter         Published IP           10.194         Configure           Published IP Range         If you want to use a Published IP Range instead of providing an Individual Published IP for each IP Range           If you want to use a Published IP Range         to	Certificate Certificate Approve (View) vCenter, enter the IP range and netmask here.	use the ter Frange. Senting up a "Debilished IP for the vCenter is optional but is required for Access Control. Published IP access can be set up after the enboarding process as well. Published IP Range A Published IP Range and be used to specify a require 10P Participation to build on all current and future vCenters in this ELM.
VCenter         Published IP           10.194         Configure           Published IP Range            If you want to use a Published IP Range instead of providing an individual Published IP for each            IP Range         to	Certificate Certificate Approve (View) vCenter, enter the IP range and netmask here.	use the ter Arange. Setting up a Published IP for the vCenter is optional but is required for Access Control. Published IP access can be set up after the onboarding process as well. Published IP Range A Published IP Range can be used to specify a range of Published IP addesses to be used for all current and future vCenters in this ELM.
VCenter         Published IP           10.194         Configure           Published IP Range         Fublished IP Range           If you want to use a Published IP Range Instead of providing an individual Published IP for each IP Range         To           IP Range         To         Netmask	Certificate Certificate Certificate Certificate Certificate Certificate	Use the ter Frange. Setting up a Vublished IP for the vCenter is optional but is required for Access Control. Published IP access can be set up after the onboarding process as well. Published IP Range A Published IP Range can be used to specify a range of Published IP Adases to be used for all current and future vCenters in this ELM.
VCenter         Published IP           10.194         Configure           Published IP Range         If you want to use a Published IP Range instead of providing an individual Published IP for each           IP Range         to           IP Range         to	Certificate Certificate Approve (View) vCenter, enter the IP range and netmask here.	use the lar Hange. Setting up a Vublished IP for the vCenter is optional but is required for Access Control. Published IP access can be stup after the enboarding process as well. Published IP Range A Published IP Range can be used to specify a range of Published IP Range can be used for all current and future vCenters in this ELM.
VCenter         Published IP           10.194         Configure           Published IP Range         If you want to use a Published IP Range instead of providing an individual Published IP for each           IP Range         to           IP Range         to           Tag Sync         Tag Sync	Certificate Certificate Approve (View) vCenter, enter the IP range and netmask here.	Use the ter Frange. Setting up a Vublished IP for the vCenter is optional but is required for Access Control. Published IP access can be stup after the enboarding process as well. Published IP Range A Published IP Range can be used to specify a range of Published IP Range can be used for all current and future vCenters in this ELM.
VCenter         Published IP           10.194         Configure           Published IP Range         If you want to use a Published IP Range instead of providing an individual Published IP for each           IP Range         to           IP Range         to           Image         to           Tag Sync         Tag Sync           Excelor         Choose whether or not to sync vCenter tags with CloudControl. This setting can be changed and the sync vCenter tags with CloudControl. This setting can be changed and the sync vCenter tags with CloudControl. This setting can be changed and the sync vCenter tags with CloudControl. This setting can be changed and the sync vCenter tags with CloudControl. This setting can be changed and the sync vCenter tags with CloudControl. This setting can be changed and the sync vCenter tags with CloudControl. This setting can be changed and the sync vCenter tags with CloudControl. This setting can be changed and the sync vCenter tags with CloudControl. This setting can be changed and the sync vCenter tags with CloudControl. This setting can be changed and the sync vCenter tags with CloudControl.	Certificate  Approve (View)  v Center, enter the IP range and netmask here.  ytime within System Jobs.	Use the ter Frange. Setting up a Vublished IP for the vCenter is optional but is required for Access Control. Published IP access can be stup after the enboarding process as well. Published IP Range Arbuished IP Range can be used to specify a range of Published IP Range can be used for all current and future vCenters in this ELM.

10. When all certificates are approved, select **Continue**.



You cannot select **Continue** until all of the Approve checkboxes are checked.

Check the online documentation instructions for more detail on Adding vCenters to CloudControl.

#### 2.6.3. View Details

On the **Details** page, you can monitor the process as all of your vSphere information is collected.

Add vCenter @ 10.194.	
1: About 👽 - 2: Configure 👽 - 3: Details - 4: Onboard Hosts - 5: Host Credentials	
Connecting to vSphere	
✓ Adding Platform Services Controllers	1 Found
✓ Adding all vCenters in ELM	1 Found
✓ Discovering Hosts	1 Found
Discovering Virtual Machines	4 Found
	Continue

#### 2.6.4. Onboard the hosts

On the **Onboard Hosts** page, you can view the hosts that were discovered, remove hosts, or add additional hosts to be added to CloudControl. Select the hosts that you want to add and select **Onboard Hosts**.



You must add hosts before you can run Configuration Hardening policies (assessment and remediation) against your hosts.

	ENTRU	IST	CloudCo	ntrol												4	?
#	🗗 vSphere		×	+ Add vCenter	×												
Add	vCenter	10.1	94.														
1: Ab	out 🖌 🗌	2: Config	ure 🗸	3: Details 🗸	4: Onboa	rd Hosts	5: Host Credentials										
The foll onboar	owing host ded can no	s were dis t be used i	covered in in any sec	n the vCenters. Se curity policy.	elect the host	s (based o	n number of available er	entitlements) t	o be onboarded.	. Once onboarde	ed, they w	vill be avai	ilable for se	curity polic	ies. Any ho	st that is	not
Filter																	
	Host					0	vCenter				Da	CI	Fo	I 0	Socket	3	
	10.194.	48.201					10.194.				Те	Те	host	10	1		
Showing	g 1 to 1 of 1	records (1	Selected)												Onbo	ard 1 F	losts
							manage Entrant Car	manufactor All Ph	white Descended								

#### 2.6.5. Host credentials

On the Hosts Credentials page, you can add or import the credentials for your ESXi hosts.

#### 2.6.5.1. Add credentials

To add credentials:

1. Select one or more ESXi hosts that share the same credentials and select the **Missing** link in the Credentials column.

2. In the **Add Host Credentials** window, enter the User Name and Password for the ESXi hosts and select **Apply**.

Edit Host C	redentials		×
Host Status Last Updated	10.194. ★ Missing - Credentials h Mar 15, 2023, 2:05:56 PM	ave not been added	
Service Acco	ount		
Provide a privile	ged service account to acce	ss the selected ESXi host.	
Service Act Add service and passwo	account Credentials	Managed Credentials Account Access service account credentials from a stored credential management account	nt
Service Accou	nt *		
root			
Service Accou	nt Password *		
			_
		Cancel Ap	ply

The **Credentials** column for each host shows the host status. This can be one of the following:

- Missing
- ° Valid
- ° Invalid



You may encounter an Invalid Certificate when adding the Host Credentials. To resolve this issue, the vCenter root CA must be imported into the CloudControl's Certificate Authorities. Check [procedures:::certificate-invalid] for troubleshooting.

#### 2.6.5.2. Import credentials

To import credentials, you must upload a CSV file in the following format: ESXINAME FQDN, PASSWORD, USERNAME:

- 1. Select one or more ESXi hosts that share the same credentials and select **Import Credentials**.
- 2. Select the file that you want to import and select Continue.
- 3. Review the summary on the **Discovered** page.
- 4. Select Apply.



If you do not add the credentials, then you cannot run Configuration Hardening policies (assessment and remediation) against your hosts.

- 5. After you have added the credentials, you can enable Global PIP. Global PIP is disabled by default. For more information, see Enable Global PIP.
- 6. Select **Continue**.
- 7. Select **Done** to view the dashboard for the newly added vCenters.



# 2.7. Enable Global PIP

- 1. From the Home tab, select Inventory > vSphere.
- 2. On the vSphere page, select the **Compute** link.

	CloudControl			= <b>▲</b>	?
# 🗗 vSphere	ж				
vSphere				🖬 Views   👻 Actions	-
Management	≣ <sup>Compute</sup> 12	# Network	≣ Storage 3	Recent Configuration Hardening Activity Assessments Remediations	× <sup>N</sup>
3	Current Configura	tion Hardening Compliant (0) Not Compliant (0)	v <sup>™</sup> ● Unassessed (3)	No assessment runs detected Vew Policies	
		Last compute	ed: Mar 15, 2023, 3:00:00 PM		

3. On the **Compute** tab, select the **Hosts** link.

	<b># &amp;</b> ?
🎄 📱 10 194 x 🕛 System Settings x 🖸 Primary Authentication x 💿 Trust Manifests x 🔊 Log Analysis x 🖉 Secondary Approval x 💋 Lisphere x	
vSphere	🖆 Views   👻 Actions   👻
@ Management: vCenters (1) 🗰 Compute (12) 🛦 Network (6) 🚍 Storage (3)	×
🗈 DataGenters (1)   📓 Clusters (1)   🖥 Hosts (1)   🖬 Virtual Machines (4)   👁 Resource Pools (1)   🛞 VApps (0)   🖿 Folders (4)	
Filter Resource Type Host System	Global PIP M Disabled Actions +
Name A OS Version o Sockets IP Address o Virtual Machines Configuration Hardening Onboard Credential	8
ID 194     ID 194	<b>№ 1</b>

4. On the Hosts page, next to the Actions button, select the Global PIP Disabled link.

Global PIP X Disabled	Actions	•
 Credentials		
✓ Valid	<b>&gt; 0</b>	

- 5. Alternatively, you can select one or more hosts and select **Actions > Manage Global PIP**.
- 6. In the Manage Global PIP window, do the following:
  - a. Set the **Status** to **Enabled**.
  - b. For Global PIP / FQDN, enter the IP address or FQDN to use for the Global PIP.
  - c. Enter the **Netmask**.
  - d. Check the **confirmation** checkbox.
  - e. Select Apply.

Manage Global PIP	×
With Global PIP, instead of individual IP addresses, one IP address is created all of your ESXi hosts. Once added to CloudControl, the hosts are automatical assigned four ports to distinguish them from other hosts. The Range of ports to be used is from 49152 to 65535.	for lly o
Making a change to the Global PIP will update the Global PIP for all ESXi hosts.	
Status ENABLED	
Global PIP / FQDN *	
10.194.	
Netmask *	
255.255.255.0	
I understand the risks of updating the Global	PIP

Cancel Apply

Global PIP is now enabled for all hosts that have been added to CloudControl.

Select **Download CSV** to download a CSV file that contains the details of all assigned ports.

Follow the online documentation to view the assigned ports for Global IP.



For more details, view the online documentation on Enabling Global PIP.

If you are not using AD, you can add local users to the system so they can be used to log in to vCenter and ESXi hosts using the Published IP address for the vCenter and GPIP for the ESXi hosts.

To create a local user to the following:

- 1. From the Home tab, select System > Primary Authentication.
- 2. Select the **Add** button.
- 3. In the Add Local User window, fill the information accordingly:

Add Local User	×
First Name *	
Test	
_ast Name *	
User	
Jser Name *	
testuser	
Must be at least 6 characters long, and can only contain letters, di characters: "-","_", "." and "@"	igits and the following special
Password *	
•••••	
A valid password must be at least 8 characters, contain at least or upper case letter, one digit and one special character.	ne lower case letter, one
Re-enter Password *	
•••••	
Groups *	
ASC_NetworkAdmin × ASC_SecurityAdmin ×	
	•
	Cancel Add

For more details, view the online documentation on Adding Local Users.

# 2.9. Test the vCenter Published IP (PIP) and ESXi Hosts Global IP (GPIP) address and ports

#### 2.9.1. vCenter Published IP (PIP)

Once the vCenter Published IP is set/enabled, you can test it by pointing your browser to:

https://PIP

#### 2.9.2. ESXi Global IP (GPIP) and ports

When you know the ports that were assigned when you enabled GPIP, you can log in to any ESXi using the GPIP and the https\_port:

https://GPIP:https\_port

#### 2.9.3. More information

Check the online documentation for more details on connecting to the ESXi hosts using the GPIP.

If CloudControl is not in AD mode, use one of the local users in CloudControl. If local users have not been created you can use the **superadminuser** local account with the password set during CloudControl configuration. Initially users must be in the **ASC\_SuperAdmin** group to be able to log in using GPIP and PIP. You can change this when you implement your own access control policy.

# 2.10. Configure email

It is important to setup your email settings so the system can provide notification to users when required. Your SMTP and email information settings are configured during installation. You can modify them at any time.

- 1. From the Home tab, select System > System Settings.
- 2. On the **System Settings** page, select **Settings > Email**.
- 3. On the Email page, select ON or OFF to enable SMTP.
- 4. Fill in the information according to your settings:

	budControl
🐇 😃 System Settings	×
System Settings	
🧿 Email 🤇	Test
SMTP Server Name or IP	Address *
XXXX.XXXX.XXXX.XXXX	
Port •	
25	
Sender*	
xxxxx@xxxxx.com	
Security	
None SSL	TLS
User Name	
Password	
Re-enter Password	

Check the online documentation for more details on how to modify your email settings.



Email notification to users is only available when Active Directory settings are enabled. This integration was performed with local users. Active Directory was not configured.

# 2.11. View the vSphere inventory

Now that the VMware inventory has been catalogued by CloudControl, check the online documentation on Viewing the vSphere Inventory inside CloudControl.

### 2.12. Logs

You can look at the logs in the system in the following places:

- 1. Log Analysis.
- 2. System Logs.

#### 2.12.1. Log analysis

Go to the Home tab, select Security > Log Analysis.

Check the online documentation for more information on log analysis.

#### 2.12.2. System logs

To view the system logs page, from the **Home** tab, select **System > System Logs**.

Check the online documentation for more information on system logs.

# 2.13. Access Control

This section will show how you can use an Access Control Policy to control access to VMware resources in the system. This example creates an access control policy that will allow anyone that belongs to the **ASC\_NetworkAdmin** or **ASC\_SuperAdmin** group to log in to ESXi hosts in CloudControl. Anyone that doesn't belong to these groups will be denied access. Keep in mind that you also can use tags to constrain the access control policy to only resources that have the specified tags.

#### 2.13.1. Users

Three users were created in the system that will allow to implement and demonstrate the access control policy in action.

() EN	ITRUST Cloud	Control										8 ?
* 8	10.194.	x () System Settings	c 💿 Trust Manifests 🛛 🛪	🔊 Log Analysis	×	2 Secondary Approval x	🛃 vSphere	×	Primary Authentication 36			
Primar	y Authentication of is in Local Authenticatio	n Mode							Config	ure Active Directory +	Ac	tions   <del>+</del>
	User ID	•	First Name		> Last N	ame	0	Groups		<ul> <li>Last Login Time</li> </ul>		٥
	testuser3		Test		User 3			ASC_NetworkEn	gineer			
	testuser2		Test		User 2			ASC_NetworkEn	gineer			
	testuser		Test		User			ASC_NetworkAd	min			
	superadminuser		Super		Admin			ASC_AuthzAdmi ASC_SuperAdmi	n			

Two users belonging to the **ASC\_NetworkEngineer**. One user belonging to the **ASC\_NetworkAdmin** group. And lastly, the **superadminuser** (which already existed) which belongs to the **ASC\_SuperAdmin** group.

#### 2.13.2. Tags

Tags will not be used in the example but here is an example of how to create a tag and assign it to a resource in the system. For instance, once assigned, you could use tags to constrain the access control policy to resources that have the tag.

Check the online documentation for more information on tags.

1. Create a tag called **ESXi\_Host**. This will be used to tag the ESXi Hosts in the system.

Create Tag 👒 ESXi_Host	2	•
1: Details – 2: Values		
Name *	Sample	
ESXi_Host	SXi_Host	
Description	128 Characters	\$
	,	1
	Cancel Continue	

- 2. Tag the ESXi Hosts with the tag created.
- 3. Now tag the ESXi Hosts in the system with the ESXi\_Host tag created.

10.194. In Test Datacenter In host I Test Cluster									
Details									
Туре	HostSystem								
Trust Attestation Status 0	Unassessed								
Virtual Machines 0									
OS Version VMware ESXi 7.0.3 build-19193900									
External ID	External ID HostSystem:host-22								
IP Address	10.194. , fe80::9e7b:efff:								
Host Credentials	✓ Valid								
Global PIP <b>1</b>	✓ Enabled (10.194. )								
Proxy Access Ports	4								
Onboarded 0	✓ Yes								
Sockets	1								
Trust Manifests	5								
Tags	SESXi_Host:True								

#### 2.13.3. Create and validate the access control policy

- 1. From the Home tab, select Security > Trust Manifests.
- 2. On the Manage Trust Manifests page, select Actions > Create Trust Manifest.
- 3. On the **Details** tab of the **Create Trust Manifest** page, enter the name and optional description for the trust manifest.
- 4. For Policy Type, select Access Control.
- 5. In the Access Control Policy section, create a rule for the NetworkAdmin Group:

Cre	ate Trust Manifest 🔐 My Access Control Policy	×
	Details YAML	
Nam	€×	
My	Access Control Policy	
Desc	ription	358 Characters
This AS(	s policy allows access to any <u>ESXI</u> Host in the system using the GPIP to only users who are in t C_SuperAdmin groups	he <u>ASC_NetworkAdmin</u> or
Polic	cy Type *	
<b>≜</b> ? /	Access Control	*
Acc	ess Control Rules	Expand All   Collapse All
~	Name *	Û
	NetworkAdmin Rule	
	Description	192 Characters
	Give access to anyone who is in the ASC_NetworkAdmin group	,
	Rule Type Choose to either allow or deny this rule. A deny rule will always override an allow rule.	
	Role * Specify the role that this rule will apply to	
	ASC_HostAdmin	-
	Subjects • Specify one or many groups and/or users that this rule will apply to	iC.
	설 [local] ASC_NetworkAdmin ×	×
	Constraints	
	Resource Tag Provides selection criteria based on tags applied to a resource	+ Add
	Subject Provides selection criteria for the user allowed to perform the action	+ Add

6. Select Add Another Rule and add the rule for the SuperAdmin group to the policy.

Name *		
Super/	Admin Rule	
Descrip	tion	194 Chara
Give a	access to anyone who is in the ASC_SuperAdmin group	
Rule Ty Choose t	pe to either allow or deny this rule. A deny rule will always override an allow rule.	
● ♥ A		
Role * Specify th	he role that this rule will apply to	
ASC_H	HostAdmin	
Subject: Specify o	ts * one or many groups and/or users that this rule will apply to	
쓭 [loc	cal] ASC_SuperAdmin ×	
Constra	aints	
Reso Provid	urce Tag des selection criteria based on tags applied to a resource	<b>+</b> Ac
Subje Provid	ect des selection criteria for the user allowed to perform the action	<b>+</b> Ac
id Anothe	er Rule	

- 7. Select **Validate** to validate the policy.
- 8. Select **Save** to save the policy.

9. Select **Publish** to publish the policy When you publish the policy it will ask you to assign resources to the policy. Select **host** and select **Assign**.

r				
Nan	ne 🔺	Vendor Type	\$ Management System 0	Trust Manifest
10.19	94.	VirtualCenter	10.194.	Inherited from parent
Appli	iance Root	Root	Self	1
datas	store	StorageFolder	10.194.	Inherited from parent
Disco	overed virtual machine	VmFolder	10.194.	Inherited from parent
host		HostFolder	10.194.	Inherited from parent
netw	rork	NetworkFolder	10.194.	Inherited from parent
Test	Cluster	Cluster	10.194.	Inherited from parent
Test	Datacenter	DataCenter	10.194.	Inherited from parent
VCLS	5	VmFolder	10.194.	Inherited from parent

#### 10. Select Close.

Check the online documentation for more details on Creating an Access Control Trust Manifest from the CloudControl GUI.

#### 2.13.4. Test the Access Control Policy

When the access control policy is in place, point your browser to the GPIP address of the ESXi host and see if you can log in.

Success:

Login should be successful for the **superadminuser** and **testuser**.

• Failure:

Login should fail for the testuser2 and testuser3 local users.

User name	testuser2	
		<b>vm</b> ware" esxi"
Password	•••••	Permission denied due to security policy
	Log in	

#### 2.13.5. Logs

You can use the Logs in the system to check why access has been denied to a user. In the example, **testuser2** has been denied access. You can view the logs to see the reasons.

1. From the Home tab, select Security > Log Analysis.

🔊 Log Ana	lysis															Retention: 1	30 days (change
Filter 🛛													🗹 Hide (	CloudC	Control view	operations (	•
- Statistics																	
6 Months   7 Da	ys 🔳 🗖 🗖						Top Users	(Las	t 7 days)								20
										superad	minuse					SYSTEM	Uta.
							Top Action	ns (La	ist 7 days)								
0						0			CloudControl.In	wentory.Edit		Auth	nenticate	Cloud	Control.Aut.	CloudCo	Unknown
							Top Resor	urces	(Last 7 days)								
Oct-22	Nov-22	Dec	-22	Jan-23	Feb-23	Mar-23				Appliance Root				10.19	14. 1	0.194.1 10.	194 Un
																	Columns *
Time		0	Priority	/	0	User		0	Action	<	R	esources		0	Status		0
Mar 17, 2023, 1	2:16:17 PM		INFO			testuser			Compute.Ho	stsystem.View	10	.194.	(HostSyste	em)	Permit		
Mar 17, 2023, 1	2:16:10 PM		INFO			testuser			Managemen	t.Administration	10	.194.	(HostSyste	im)	Permit		
Mar 17, 2023, 1	2:16:10 PM		O INFO			testuser			Compute.Ho	stsystem.Login	10	.194.	(HostSyste	im)	Permit		
Mar 17, 2023, 1	2:16:10 PM		O INFO			testuser			Authenticate		h	z8esxi.	(Host		Permit		
Mar 17, 2023, 1	2:16:05 PM		A WAR	N		testuser3			Compute.Ho	stsystem.Login	10	.194.	(HostSyste	em)	Deny		
Mar 17, 2023, 1	2:16:05 PM		INFO			testuser3			Authenticate		hj	z8esxi.	(Host		Permit		
Mar 17, 2023, 1	2:15:59 PM		🛦 wari	N		testuser2			Compute.Ho	stsystem.Login	10	.194.	(HostSyste	ım)	Deny		
Mar 17, 2023, 1	2:15:58 PM	(	O INFO			testuser2			Authenticate		h	z8esxi.	(Host	t	Permit		

2. Select the record that shows the **Deny** status to see the reason for the denial.

🛕 Mar 17,	2023, 12:15:59 PM				15 of 10645 🔕 😒 🗙
		Details	Payload	Related Logs (0)	
Authorization d There needs to	enied due to no rules applying to the use be at least one direct role association by	r via the o way of us	configured ser name o	access control p r group(s)	olicy for the resource(s) with name(s) '[10.194. ]'.
Privileges	Compute.Hostsystem.Login			Date	Mar 17, 2023, 12:15:59 PM
Resources	10.194. (ESXi)			Priority	A WARN
Source	Unknown (10.194. )			Status	Deny
Destination	cloudcontrol660hpz8. (10.194.	)		User	testuser2
Protocol	vSphereHostClient			Groups	
Policy	Enforced			Roles	
Msg ID	AUZ0001			Action	Compute.Hostsystem.Login
Category	AUZ			Vendor Action	Login
				Trust Manifest	My Access Control Policy

3. You will be able to see the My Access Control Policy was used to control the access.

# 2.14. Secondary Approval

Use Secondary Approval to configure CloudControl to require additional approval before users can perform selected disruptive operations on a resource. For example, you can require secondary approval before deleting or powering off a virtual machine or vApp, editing a firewall, or creating an Edge gateway service.

When a user attempts to perform a vSphere operation that requires secondary approval, the operation fails with a notification that secondary approval is required, and that a request was generated.



If you have SMTP configured, and the users or groups have an email address in AD, then email messages are generated.

This example will require the user **testuser** a secondary approval to log in to any ESXi host.

# 2.14.1. Create a Secondary Approval Trust Manifest from the CloudControl GUI

- 1. From the Home tab, select Security > Trust Manifests.
- 2. On the **Manage Trust Manifests** page, select **Create Trust Manifest** (The Plus sign in the GUI).
- 3. On the **Details** tab of the **Create Trust Manifest** page, enter the name and optional description for the trust manifest.
- 4. For Policy Type, select Secondary Approval.

Create Trust Manifest 👲 My Secondary Approval	×
	Details YAML
Name *	
My Secondary Approval	
Description	477 Characters
Test Secondary Approval	
Policy Type *	
2 Secondary Approval	<b>▼</b>

- 5. In the Secondary Approval Policy section, complete according to the image below:
  - a. Select the **testuser** as the subject.
  - b. Select the **superadminuser** as the approver.
  - c. Select the Compute.Hostsystem.Login as the operation.

Name *		
Second	dary Approval Rule	
Descript	tion	246 Chara
test		
Cubicat		
Subjects Specify w	8 * who needs secondary approval to perform the given operations.	
🛔 [loca	alj testuser x	
Approve	ers *	
Specity w	no needs to approve the secondary approval requests.	
Operatio Add abstr	ons * ract operations that must be approved in order to perform, ufe Hostsystem.Login *	X
Add abstr Comput Approva Once app	ons + ract operations that must be approved in order to perform.	× -
Add abstr Comput Approva Once app 120 Max Allo Set the m	ons * ract operations that must be approved in order to perform.	X -
Operatio Add abstr. Comput Approva Once app 120 Max Allo Set the m Constrai	ons * irract operations that must be approved in order to perform.	X -
Operatio Add abstr. Comput Approva Once app 120 Max Allo Set the m Constrai Resou Provide	ons • ract operations that must be approved in order to perform.  dire.Mostsystem Login ×  al Duration proved, the amount of time in which the subject can perform the approved operations.  Minutes  Minutes  word Operations nax: number of operations allowed during the approval time window. Leave blank for unlimited.  ints  wore Tag Bes selection oriteria based on tags applied to a resource	× - + At
Operatio Add abstr. Comput Approva Once app 120 Max Allo Set the m Constrai Resou Provide Subjet Provide	ons + ract operations that must be approved in order to perform.  dire.Hostsystem Login ×  al Duration proved, the amount of time in which the subject can perform the approved operations.  Minutes  word Operations nax number of operations allowed during the approval time window. Leave blank for unlimited.  mints urce Tag les selection oriteria based on tags applied to a resource  ct tes selection criteria for the user allowed to perform the action	× - + Ad + Ad

- 6. Publish the policy.
- 7. When you publish the policy you must assign resources to it. Select **host** as the resource. This will make policy applicable to any ESXi host in the system.

#### 2.14.2. Validate Secondary Approval Policy

When the secondary approval policy is in place, point your browser to the GPIP address of the ESXi host and see if you can log in. Log in with the user that you used in the policy definition. The attempt should fail.

#### 2.14.3. Approve the secondary approval request

Approve the secondary approval so that the user can log in to the ESXi Host.

- 1. From the Home tab, select Security > Secondary Approval Requests.
- 2. On the Secondary Approval Requests page, select a tab to view Pending or All requests.

<b>()</b>		CloudCon	itrol														4	?
#	🛃 vSphere	× 🛃 10	.194.	х	10.194.	х	() System Settings	×	Primary Authenti	0	Trust	Manifests	×	🔊 Log Analysis	×	2 Secon	ndary App	r X
Seco	ndary Approva	l Requ	ests				Pend	ling	All									
Filter													C	Hide expired 🚯		Deny	Арр	prove
	Request Time		Reques	tor	0	Reso	urce	0	Operation		0	Approvers		0	Expira	tion Time	)	0
	Mar 17, 2023, 12:26	40 PM	testuser			10.19	94.		Compute.Hostsystem.Log	gin		1			Mar 17,	2023, 2:26	:40 PM	

3. (Optional) Select Approve for a pending request to approve the request.

Pending Reques	t		×
Request Time	Oct 20, 2021, 9:03:26 AM		
Requestor	testuser		
Resource	10.194		
Operation	Compute.Hostsystem.Login		
Approvers	SuperAdminUser		
Max Allowed Operations	Unlimited		
Approval Duration	2 Hours		
	Cancel	Deny	Approve

Approve Pending Request

X

	<b>J</b> · · · · <b>J</b> · · · · ·	
Request Time	Mar 17, 2023, 12:26:40 PM	
Requestor	testuser	
Resource	10.194.148.201	
Operation	Compute.Hostsystem.Login	
Approvers	💄 superadminuser	
Max Allowed Operations	Unlimited (Change)	
Approval Duration	2 Hours (Change)	
Start Time Window Time to start the window window is based on the	that user can perform approved opera approval duration	tion. Length of the
Mar 17, 2023, 12:2	7:46 PM	× 🛍
	Cana	
	Canc	Approve

4. (Optional) Select **Deny** for a pending request to reject the request.

#### 2.14.4. Attempt to log in after approval

After the secondary approval request is approved, log in:

Point your browser to the GPIP address of the ESXi host and see if you can log in. Log in with the user that you used in the policy definition. The attempt should be successful.

### 2.15. Configuration Hardening

Configuration hardening allows you to improve the security posture of your vSphere environment by hardening the configuration to meet either your company's specific security policy, industry best practices such as CIS or NIST, or compliance standards such as PCI or HIPAA. By automating the hardening process, you can reduce your operational burden during a compliance audit.

With CloudControl, you can:

- Create and customize templates to use in configuration hardening checks.
- Assess and remediate your environments against the configuration hardening checks defined in the templates.
- Review dashboards, reports and alerts to monitor the results of assessments and remediations.

#### 2.15.1. About Templates

CloudControl uses templates to support all Configuration Hardening activities. CloudControl supports the following types of templates:

- **Catalog templates**—Read-only collection of hardening operations. There is a vSphere operations catalog of templates that you can use.
- **System templates**—Read-only collection of operations derived from a catalog template for a given compliance standard For example, the vSphere HIPAA Security Standards template is derived from the vSphere operations catalog template.
- **Custom templates**—Templates created by users. In most cases, they are copied or cloned from existing system or catalog templates. Custom templates can be modified and used in configuration hardening policies.



CloudControl also includes sample custom templates that can immediately be used in a policy.

Templates can contain both assessment and remediation hardening operations. It is recommended that you review all operations in the template to ensure that any parameter values are set to those that appropriate for your infrastructure requirements.

#### 2.15.2. About Policies

Configuration Hardening Policies are used to run custom templates. Each policy associates a template with one or more resources or tag-based resource configurations, and can be run manually or as a scheduled activity. Policies can either assess or remediate a resource, but cannot do both.

#### 2.15.3. More information

Consult the online documentation for more information on Configuration Hardening.

#### 2.15.4. Creating a Configuration Hardening Policy Example

For this guide a configuration hardening policy will be created based on one of the templates available. Enforcement will be based on a rule in the template to check and make sure the ESXi vSphere version is at least version 7 and above.

- 1. From the Home tab, select Security > Configuration Hardening.
- 2. On the Configuration Hardening Management page, select the Policies tab.

- 3. Select the Create (+) button.
- 4. In the **Create Policy** wizard on the **Select Type** page, select the type of policy that you want to create. This can be one of the following:
  - Assess Only Runs operations on the host to compare the parameter values specified in the template with the actual values on the host.
  - Remediate Only Modifies the parameter values on the host in order to match the values specified in the templates.
- 5. Select Assess Only.

Create Policy ©	×
1: Select Type - 2: Details - 3: Templates - 4: Resources - 5: Schedule	
Assess Only Assessment is the process of running operations, or tests, on the resource to compare the parameter value specified in t template with the actual value configured on the resource.	ihe
Remediate Remediation modifies parameter values on the resources based on the desired values defined in templates. Will only run remediation on operations that are selected for remediation.	1
Ca	ncel Continue

- 6. Select Continue.
- 7. On the **Details** page, enter the name and optional description of the policy, and specify whether the policy is enabled.

Create Policy		×
1: Select Type ✔ - 2: Details - 3: Templates - 4: Resources - 5: Schedule		
Name •		
My Configuration Hardening Policy		
Status Develue		
Description 210 Characters		
This is a test configuration hardening policy		
Back	Cancel	Continue

- 8. Select Continue.
- 9. On the **Templates** page, select the **resource type** for the policy. This can be one of the following:
  - ° AWS Account Runs AWS-related templates against your AWS environment.
  - ° ESXi Runs vSphere related templates against your ESXi hosts.
  - Kubernetes Runs Kubernetes related templates against your Kubernetes environment.
  - **NSXDataCenter** Runs NSX-T related templates against your NSX-T environment.

- 10. Select **ESXi** as the template to run against your environment.
- 11. The template list displays the name, description and type of operations Select a template that contains the type of operations that you selected for the policy.
- 12. Select vSphere HyTrust Best Practice template. This template is used in the example.

Creat	Re Policy S My Configuration H	ardening Policy					×
1: Sel	ect Type 🖌 — 2: Details 🖌 —	3: Templates – 4: Assignmen	ts	5: Resource Constraints	6: Schedule	2	
Resou	rce Type						
ESXi							~
Select The used	t a Template by VSphere - HyTr following is a list of templates for th in this policy.	ust Best Practice with HyTrust di e selected resource type. If a sy	efault stern	values template is selected, a cli	one of the templa	te will be created and	d
	Template Name \$	Description	\$	Type 🗘	Operations	5	
	vSphere - HyTrust Best Practic	This template is based on Hy	Tr	Custom	70 Assess, 66	Remediate	
	vSphere - Configuration Template	This template consists of ope	ra	System	45 Assess, 45	Remediate	
	vSphere 7.0 - VMware Security	This template contains all the	0	System	105 Assess, S	94 Remediate	
	vSphere - PCI Data Security St	Payment Card Industry Data	S	System	146 Assess, 1	36 Remediate	
	vSphere - VM - DISA STIG 6.7	DISA VMware vSphere Versio	on	System	22 Assess, 21	Remediate	
	vSphere - VM - DISA STIG 6.0	DISA VMware vSphere Versio	on	System	42 Assess, 41	Remediate	
	vSphere - NIST SP 800-53r5	NIST Special Publication 800	-5	System	161 Assess, 1	153 Remediate	
Showing Back	1 to 8 of 17 records (1 Selected)	**** I I I I I I I I		· ·	05 A	Cancel Continu	▼ ue



See the online documentation for more information on Creating a Custom Template.

- 13. Select **Continue**.
- 14. On the **Assignments** page, select one of the following and choose what resources to which you want to apply the policy:
  - Tags Select the Tags radio button and then choose a tag or tags assigned to the resource. Select the + icon if you want to assign more tags to the resource. If there are no tags assigned, you can select the Assign Tags Now link.
  - ° Resources Select Specific Resources and then choose one or more resources.

For vSphere only, you can choose a parent for the resource type. This can be one of the following:

- vCenter Allows you to select all ESXi hosts in the selected vCenter. All onboarded ESXi hosts in the selected vCenter will be considered for hardening. You can select multiple vCenters. When the Configuration Hardening policy is run, CloudControl retrieves all onboarded ESXi hosts from the vCenter inventory to ensure the list of ESXi hosts is always current.
- Appliance Root Allows you to select all ESXi hosts under Appliance Root. All onboarded ESXi hosts will be considered for hardening. When the

Configuration Hardening policy is run, CloudControl retrieves all onboarded ESXi hosts from the vCenter inventory to ensure the list of ESXi hosts is always current.

- DataCenter Allows you to select all ESXi hosts in the selected DataCenter. All onboarded ESXi hosts in the selected vCenter will be considered for hardening. You can select multiple DataCenters. When the Configuration Hardening policy is run, CloudControl retrieves all onboarded ESXi hosts from the vCenter inventory to ensure the list of ESXi hosts is always current.
- Cluster Allows you to select all ESXi hosts in the selected Cluster. All onboarded ESXi hosts in the selected Cluster will be considered for hardening. You can select multiple Clusters. When the Configuration Hardening policy is run, CloudControl retrieves all onboarded ESXi hosts from the vCenter inventory to ensure the list of ESXi hosts is always current.
- ESXi Host Allows you to choose which individual ESXi hosts that you want to use as a resource. If additional ESXi hosts are onboarded, they will not be included.
- 15. Select **Tags** for the resources you want to apply the policy.
- 16. Select the Assign Tags to Policy Now link to select the tags.

Create Policy <sup>(i)</sup> My Configuration Hardening Policy			×
1: Select Type 🖌 - 2: Details 🖌 - 3: Templates 🖌 - 4: Assignments - 5: Resource Constrain	nts 6	: Schedule	
Assign this policy to one or more ESXi Hosts based on tags, by resource or by direct assignment.			
Tags     Apply this policy to ESXI Hosts that have the following tags     Apply this policy to either a reso	urce or in	dividual ESXi ho	osts
Assigned Tags to this Policy			
Filter		Assign	n Tags 📋
Tag Name $\diamond$ Value $\star$ Source $\diamond$ Description	٥	ESXi Host	ts ≎
No tags are currently assigned to this policy			
Assign rays to rolly, now			
No records were found			
Back		Cancel	Continue

#### The Assign Tags dialog appears.

17. Select the **ESXi\_Host** tag created earlier.

Grant	Annie												
Creat	Assi	gn lags										~	~
1: Sele	🕜 The	policy will be assigne	ed to re	sources wi	th the following s	elected	tags and valu	es.					
Assign ti	1: Se	lect Tag – 2: Values	5										
Ti Al	Filter										Create Ta	g	
		Name	•	Type ≎	Source	0	Descri	0	Values	٥	Resources	0	
Assigr		SESXi_Host	(	Custom	Appliance Cons	ole	Used to ta		1		1		
Filter													•
													<u> </u>
No record													
Back	Showing	g 1 to 1 of 1 records (1	Selecte	d)									ntinue
										Cance	Continu	ie	

- 18. Select Continue.
- 19. Select the Tag value **True** that applies to the **ESXi\_Host** tag.

Assig	gn Tags 🔖 ESXi_Ho	ost					3
7 The	policy will be assigned t	o res	ources with the following	j sele	ected tags and values.		
1: Sel	lect Tag 🖌 – 2: Value	2S					
ilter							
	Value	•	Source	٥	Description 0	Resource	s ¢
	True		Appliance Console		True states the object	1	

20. Select Assign.

Back

21. Select Continue.

Showing 1 to 1 of 1 records (1 Selected)

22. (Optional) For vSphere only. On the **Resource Constraint** page, choose which tagbased resource constraints that you want to use for your ESXi hosts. This option is not described in detail.

Cancel

Assign

23. Select Continue.

24. On the Schedule page, select if you want to enable a recurring schedule.

If enabled, select the type of schedule that you want to use to run the policy, and then specify the start date. This can be one of the following:

- Daily The policy will run every day at the time that you specify.
- **Hourly** The policy will run periodically throughout the day, based on the schedule you define.
- **Weekly** The policy will run on every day that you select at the time that you specify.

Create Policy										
1: Select Type 🖌 - 2: Details 🖌 - 3:	Templates 🖌 🚽 4: Assignments	✓ - 5: Resource Constraints ✔	6: Schedule							
Recurring Schedule										
Status ENABLED										
Frequency										
Daily		*								
Every day at 09 : 00 AM										
Start Date										
Today	<u> </u>									
Back			Cancel Create							

#### 25. Select Create.

26. The newly created policy will be displayed on the **Policies** tab.

e ا	NTRUST Clo	udControl												1	:	4	?
Config	uration Harden	ing Manager	nent			Policies T	empl	ates				G	lobal Complian	e Thre	ishold:	100% (	change)
Filter													- +	Û	A	ctions	
															(	Colum	ns 🕶
	Name	•	Description	0	Template		0	Resource Type	0	Schedule		0	Last Event	0	Stat	us	0
	My Configuration	Hardening Policy	This is a test configuration h	harde	vSphere - HyTrust	Best Practice		ESXi		Daily at 09:00 A	М				ENA	BLED	

27. Edit the **Check ESXi Patch Version** Rule in the template. Select the **vSphere - HyTrust Best Practice** link in the **Template** Column. The template details appears.

VSphere - HyTrust Best Practice with Custom	HyTrust default values						🛛 Views   - Actions	•
	Operations Severity Summary				Details			
33 нісн	23 LOW	Description Template Type Resource Type Assigned Status Created Updated	This simplifie is based on HyThot Birst Practices for vigbarre platform and contains HyTho default visited for parameters Exotom Exot I to Us Mur 15, 2023, 12-42:00 PM Mur 15, 2023, 12-42:00 PM			and contains HyTrust defined		
			70 Total Operations	68 Configured	Summary of Operation	ns 66 Remediation	1 Remediation Disabled HIGH	~
1 Mar 15, 2023, 12:42:00 PM	Revisions	System	ID: 02 ASC Operation ID: Disable Copy and Pa ID: 03 ASC Operation ID:	ASC-vSphere-0002 ste Operations in VI ASC-vSphere-0003	M Console		LOW	1
			Limit Virtual Machine ID: 04 ABC Operation ID: Limit Informational M ID: 05 ABC Operation ID:	Log File Size and N ASC-rSphere-0004 essages From VM to ASC-rSphere-0005	umber o VMX File		LOW	¥

28. Under Summary of Operations look for Check ESXi Patch Version.

#### Check ESXi Patch Version

ID: 02 ASC Operation ID: ASC-vSphere-0002

29. Once you find it, select the Check ESXi Patch Version link to edit the rule.

Operation	check ESXi Patch Version
	Details Params Remediation Steps
ID	02
Description	By staying up to date on ESXi patches, vulnerabilities in the hypervisor can be mitigated. An educated attacker can exploit known vulnerabilities when attempting to attain access or elevate privileges on an ESXi host.
ASC Operation ID	ASC-vSphere-0002
ASC Operation Name	vsphere-esxi-check-patch-version
Version	vSphere SCG-6.5u1
Category	Compute
Resource Type	ESXi
Created	Oct 12, 2021, 1:42:08 PM
Operation Source	vSphere Security Configuration Guide
Reference	https://pubs.vmware.com/vsphere-65/topic/com.vmware.vsphere.update_manager.doc/GUID- D53B8D36-A8D7-4B3B-895C-929267508026.html 🕜
Action	Assess Only
Status ENABLED	
Custom Notes	4096 Characters
Severity	
High	<b>•</b>
	Cancel Save and Close Save

30. Select the **Params** tab and enter the version according to the image below.

Operation	Check ESXi Patch Vers	Version						
		Details	Params	Remediation Steps				
version *								
VMware ESX	l 7.* build-*							
omma separated li ersion and Build N	st of ESXi patch levels. Pato umbers. Example - 'VMware	h level forma ESXI 6.* bui	t: 'VMware E Id-*' will allow	SXi <version> build-<bui all 6.x version and build.</bui </version>	d Number>'. '*' can be used to allow si	milar		

#### 31. Select Save and Close.

Now when the Configuration Hardening Policy runs, this rule will check to see if the version of the ESXi Host will match what is on the version field of the rule.

Cancel

Save and Close

Save

When you run a remediation policy, the assessment policy will automatically run immediately following its completion. This ensures that your compliance score is updated with the new percentage.

- 32. From the Home tab, select Security > Configuration Hardening.
- 33. On the Configuration Hardening Management page, select the Policies tab.
- 34. Select the Policy that you want to run.
- 35. Select Actions > Run Now.
- 36. In the confirmation window, select **Run Now**.

٢	ENT	RUST CloudControl										■ ▲ ?
#	QC	infiguration Hardeni 🕱										
Con	Configuration Hardening Management Policies Templates Global Compliance Threshold: 100% (dwarph)											
Filter												+      Actions
												Clone Policy
		Name	Description	0	Template	(	Reso	urce Type	0	Schedule	0	Run Now
	0	My Configuration Hardening Policy	This is a test configuration hard	e	vSphere - HyTrust Best Pra	ctice	ESXi			Daily at 09:00 AM		Terminate

- 37. You can view the results by selecting the link in the Last Event column.
- 38. Select View Full Results.

() EN		CloudControl											- 4	?
# 8	0.194.	🗴 🕛 System Setting	ps x 🕲 Trus	t Manifests x	🔊 Log Analysis	x _Q Secon	adary Approval 🗙	🛃 vSphere	×	Primary Authentication x	O Configuration Hardeni	× 🖹 vSj	shere - HyTrust	Ве ж
Config	uration Harde	ening Managemen	it			Policies	s Templates				Gioba	Complian	e Threshold: 10	00% (change)
Filter													a Ad	tions   +
													Co	olumns -
	Name	0	Description	0	Template	0	Resource Type		0 Sched	iule	C Last Event	•	Status	0
. 0	My Configuratio	n Hardening Policy	This is a test configu	ration hardenin	vSphere - HyTrust Best Pra	ctice wit	ESXi		Daily a	09.00 AM	Mar 17, 2023, 12:55:57	PM	ENABLED	
										Last Ev 1 Compl Policy Template Resource Byped 1 View Fu	nt Summary ttely scanned @ Not scanned My Configuration I: Policy vSphere - HyTrust B with HyTrust defaul Type ESXI II Results	i values	e* ₩ 0	

39. In the Last Event Summary Tab, select Resource.



If you used resource constraints on your ESXi hosts, you can see which hosts were analyzed and which were skipped.

i

40. As you look to the results, you will be able to see that the ESXi Version test that was in the policy, **Passed**.

Passed	Check ESXi Patch Version ID: 02 ASC ID: ASC-vSphere-0002 Assessment Time: Mar 17, 2023, 12:55:53 PM Category: Compute Elapsed Time: < 1 second Resource Type: ESXi Version: vSphere SCG-6.5u1
	Result
	ESXi patch level already matches at least one of the patterns provided, Current VMware ESXi 7.0.3 build-19193900 and Expected patterns: VMware ESXI 7.* build-* (More details) (Remediation Steps)

If you enter the incorrect version in the Check ESXi Patch Version Params, the Configuration Hardening Policy will catch the failure. For example, if you enter VMware ESXi version 8 instead of 7:

Operation Check ESXI Patch Version										
		Details	Params	Remediation Steps						
version *										
VMware ESXI 8.* build-*										
Comma separated list of ESXi patch levels. Patch level format: "VMware ESXi <version> build-<build number="">". "*' can be used to allow similar Version and Build Numbers. Example - "VMware ESXI 6." build-" will allow all 6.x version and build.</build></version>										

When you run the Configuration Hardening Policy, the system will catch the error and report a failed result.



# 2.16. Remediation Policy

Now that the Configuration Hardening Policy has been created, the same process will be used to create a Remediation Policy. The process is basically the same, with the exception that instead of selecting **Assess Only** as the type, the **Remediate** type will be selected

#### during the policy creation process.

Create Policy Ø	×
1: Select Type – 2: Details – 3: Templates – 4: Resources – 5: Schedule	
Assess Only     Assessment is the process of running operations, or tests, on the resource to compare the parameter value specified in the template with the actual value configured on the resource.	
Remediate Remediation modifies parameter values on the resources based on the desired values defined in templates. Will only run remediation on operations that are selected for remediation.	
Cancel Con	tinue

After the policy is created, edit the policy template to contain only the items you want to remediate.

You do this in the **Configuration Hardening Management** page, by selecting the template in the **Template** column of the policy you want to edit. On the **Template** page, under the **Summary of Operations**, select **Total Operations**. The **Manage Operations** page appears. This page is used to select the rules that you want in the template. You can also **Add** and **Delete** selected rules.

Now that the template has been defined with the wanted rules, perform the remediation. This example shows how to **Disable SSH** on the ESXi host just by running the remediation policy.

The following rules are in the template. (One of them is **Disable SSH**).

Matches Found (6)	Sort b	Name		1.	
0 Selected					1
Audit Exception Users List     D: 12: ASC Operation 1: Asception users list     De to 2: ASC Operation 1: Asception to the Section of th	nt more			н	IGF 4
Check ESX Patch Version D: 02 ARC persion D: ACM-object-solucy D: 02 ARC persion D: ACM-object-solucy D: 02 ARC persion D: ACM-object-solucy D: 02 ARC persion D: 92 ARC pers	in more			н	IGł
Check Local Accounts on ESXI Host D. 67 ASC Operation D. ASC-dpiewe0007 Develoption: Developtio			e : A Remed	H lot Config lation Disa	IGH junex ablex
Disable ESXI Shall     D: 11 ASC Operation TX. ASC-register-6011     D: 11 ASC Operation TX. ASC-register-6011     Decentifies: ESXI Shall as interactive command line environment available from the DCUI or remotely via SSH. Access to this mode requires the root passend of the server. The EDXI Shall can be lumed on and or Reacoust Type: ESXI Catagory: Compad. Version: ESXI Version STI'S	ff f more			MED	IUN
Disable SSH D 12 ASC Operation ID. ASC-dptwe-6011 Decodings: SSH is stable by default. BSX The use of SSH to an ESX host should be limited in scope and use. SSH enablement is controlled via the SSH service. This service is stopped by default. Rescurse Type: ESX Category: Compute Vision (dystwer SOC4.551: Action: Assess and Remediate Created: Cett 2, 201; 19:22-FM Used: Cett 19:20-11794 Decodings: Cett 19:20-11794 Decod				н	IGł
Verify PCI Passthrough D: 75 ASC Centrol D: ASC-Aspense 6075				н	IGł

Before running the policy, go to the ESXi Host and validate that SSH service is running.

	in all environments		C & Adr	ninistrator@HPZ8. 🗸	© ?~.
<ul> <li>         Image: Second secon</li></ul>	E 10.194. : ACT Summary Monitor Configure Authentication Services Certificate Power Management	e Permissions VMs Dataste Services restart start stop et	DIT STARTUP POLICY		REFRESH
Image: 10.194.     Image: 10.194.       Image: 10.194.     Image: 10.194	Advanced System Settings System Resource Reservati Firewall Services	Name           Direct Console UI           ESXi Shell	Daemon     Running     Stopped	Startup Policy Start and stop with host Start and stop manually	
	Security Profile System Swap Packages Hardware  V	SSH     attestd     dpd     kmxd	Stopped Stopped Stopped	Start and stop manually Start and stop manually Start and stop manually Start and stop manually	

Run the remediation policy and see what happens to SSH in the ESXi Host.

In the Entrust CloudControl VM do the following:

- 1. From the Home tab, select Security > Configuration Hardening.
- 2. On the Configuration Hardening Management page, select the Policies tab.
- 3. Select the remediation policy that you want to run.
- 4. Select **Actions > Run Now**.
- 5. In the confirmation window, select **Run Now**.
- 6. Once it finishes running, you can view the results by selecting the link in the Last Event column.

<b>()</b> =	NTRUST	CloudControl															4	?
# 1	10.194	× 🕛 System Se	ettings	🗙 🎯 Trust Manifests	х	🔊 Log Analysis 🛛 🗙 🛓	🛛 Seo	ondary Approval 😠	evs)	ohere		x 🔄 Primary Authentic	ation x	O Configuration Hardeni 1	< 🗈 🕯	/Sphere - HyTr	ust Be	ж
Confi	guration Hard	ening Managen	nent			1	Polici	es Templates						Global	Complia	ance Threshold	100% (	change)
Filter														/	+	•	Actions	-
																	Colum	ns -
	Name		0 1	Description	0	Template	¢	Resource Type			0 Sc	chedule		<ul> <li>Last Event</li> </ul>		<ul> <li>Status</li> </ul>		0
	My Configurati	n Hardening Policy		his is a test configuration hardenin		vSphere - HyTrust Best Practice v	wit	ESXi			Da	aily at 09:00 AM		Mar 17, 2023, 12:55:57 F	м	ENABLE	0	
	My Remediation	n Policy		This is a test remediation policy		vSphere - HyTrust Best Practice v	wit	ESXi			Da	sily at 09:00 AM		Mar 17, 2023, 1:07:52 Pl	N	ENABLE		

7. Locate the **Disable SSH** result and validate that it **Passed**.

😨 Last Event Summary		×	×
I Policy My Rem Template vSphere Resource Type ESXI	Resource         Image: 10,104.           Policy         My Remediation Policy         Policy Type         Remediate           Template         vSphere - Hy Trust Best Practice with         Template Relision         2           Template         VSphere - Hy Trust Best Practice         Elapsed Time         65 seconds		8:55 PM
Total Resources (1) 1 Completely scanned (1 Updated)	Time Mar 17, 2023, 1:07:52 PM Vendor Resource Type ESXi Operations (70 Total)		
Filter	Passed 65 (93%) (41 Updated) Failed 1 (1%) Skipped 4 (6%)		
Resource 0 1	Filter Sort by Operation Name	• •	≎ Status ≎
10.194. N	Version: Vsphere SCG6 5u1 Result T.S. protocol parameter is configured correctly, current ssV2,fsV1,fsV1,f, expected scd.18u7 ft bits / 1.f. doer default informations Strond	٥ •	✓ COMPLETED
	Disable SSH     Disable SSH     Or 12 AC: 0. AC-/sghee-0012 Assessment Time Mar 17, 2020, 107:01 PM     Origin / Sgheer SCG-6 Sut     Version / Sgheer SCG-6 Sut     Version / Sgheer SCG-6 Sut     Version / Subter	HIGH	
1 records	Disable Tools Auto Install     Disable Tools Auto Install     Disable Tools Auto Install     Disable Tools Auto Install     Category Compute Elapsof Time: I seconds Resource Type: VirtualMachine     Version: Vostore Stafe Stafe	LOW	난 Download Summary Close
cted)	70 Records 止Download	Close	

8. Now go back to the ESXi Host and check if the SSH service is running. It should be set to **Stopped**.

$\equiv$ vSphere Client Q Search						)~
<ul> <li>()</li> <li>(</li></ul>	10.194. : Acc Summary Monitor Configur Authentication Services Certificate Power Management	e Permissions VMs Datastores Network Services RESTART START STOP EDIT STARTUP POLIC	s Updates		REFRESH	<sup>ב</sup>
10.194. Cctestvm1 hpz8vcenter vmtoencrypt	Advanced System Settings System Resource Reservati Firewall Services Security Profile	Name         Y           O         Direct Console UI           O         ESXI Shell           O         SSH	Daemon Running Stopped Stopped	Startup Policy Start and stop with host Start and stop manually Start and stop manually		
	System Swap Packages	O dpd	Stopped Stopped	Start and stop manually Start and stop manually		

This example shows how you can use the remediation policy to automatically enforce configuration settings on your vSphere environment.

# Chapter 3. Troubleshooting

The following are errors that might appear during the procedures described in this guide.

# 3.1. Host Credentials: Certificate Invalid

When adding the host credentials you may encounter the error **Host Credentials: Certificate Invalid**. For example:

	dControl
A 🗗 vSphere	Primary Authenticat X 🛃 10.194. X
10.194.	Datacenter 🍗 host 🟢 Test Cluster
	Details
Туре	HostSystem
Trust Attestation Status 1	Unassessed
Virtual Machines	4
OS Version	VMware ESXi 7.0.3 build-19193900
External ID	HostSystem:host-22
IP Address	10.194. , fe80::9e7b:efff:
Host Credentials	X Certificate Invalid
Global PIP 0	X Disabled
Proxy Access Ports	<u>▲</u> 0
Onboarded 🖲	✓ Yes
Sockets	1
Trust Manifests	5
Tags	Assign Now

To resolve this issue, the vCenter root CA must be imported into the CloudControl's Certificate Authorities:

1. Launch a Linux Terminal and use **openssl** to pull the root CA from vCenter. Where it shows IP, enter the vCenter IP address.

% echo | openssl s\_client -connect <IP>:443 -showcerts

2. Enter the commands below to view the certificate:

```
% curl -k https://<IP>/certs/download.zip -o
% root_ca.zip
% unzip root_ca.zip
% cd certs
% cd lin
% cat 93a87255.0
```

3. Copy the certificate from the cat 93a7255.0 command. Start from -----BEGIN CERTIFICATE----- and end with -----END CERTIFICATE-----.

- 4. Login to your Cloud Control node as superadminuser.
- 5. From Home, select System > System Settings > Settings Drop-Down Menu > Certificates.

() e	NTRUST CloudControl							4	?
* 6	vSphere 🗙 🛃 10.194.	🗶 🔝 Primary Authentication 🗶	U System Settings X	10.194.	×				
Syster	m Settings				🗘 Settings 🗸	Views	· /	Actions	•   •
		Services	Certificates	<ul> <li>Ⅲ DNS</li> <li>④ Email</li> <li>④ Date &amp; Time</li> <li>△ Licensing</li> </ul>					×
Filter	Certificate Owner (Subject DN)	Certificate Issuer		Certificates		Expires		•	۵
	subject= C = US, CN = 10.194.148.12	issuer= OU = VMware Engineer	ing, O = localhost, ST = Californ	ia, 👳 Web Proxy		Mar 15 04:30:32	2025 G	MT	
	subject= OU = VMware Engineering, O = localho	issuer= OU = VMware Engineer	ing, O = localhost, ST = Californ	ia, Credentials	Management	Mar 9 16:30:28 2	033 GN	ΛT	
	subject= emailAddress = vmca@vmware.com, C	issuer= OU = VMware Engineer	ing, O = localhost, ST = Californ	ia,	st inneritance	Mar 13 16:44:13	2028 G	MT	

- 6. Select Certificate Authorities.
- 7. Select Add on the top right.

The Install Certificate page appears.

8. Select Enter Text and paste the certificate.

Install Certificate	×
Import Enter Text	
Certificate Data	
<pre>BEGIN CERTIFICATE MIIE0jCCAwqgAwIBAgIJAOscS7EjfiQMA0GCSqGSIb3DQEBCwUAMIGNMQswCQYD VQQDDAJQDTEUMBLGCgmSJomTBixkARkkWBGhwejgxFTATBg0JkiaJk/IsZAEZFgVs b2NhbDELMAkGA1UEBhMCVVMxE2ARBgNVBAgMCkNhbGlmb3JuaWExEJAQBgNVBAM CWxvY2Fsa092dDEbMBkGA1UECwsSVk13YXJIIEVu22luZWVyaWSnMBAXDTIAMDMx NDESNDUIMVoXDTI4MDMxHzESNDUIMVowgZ6xCzAJBgNVBAYTAIVTMRMwEQYDVQQI DApDYWxpZm9ybmlhMRIwEAYDVQQHDA1QYUxvIEFsdG8xDzANBgNVBAMBIZNdZFy ZTEbMBkGA1UECwsSVk13YXJIIEVu22luZWVyaWSnMRcwFQYDVQQDA4xMC4xOTQu MTQ4LjIwMTEeMBwGCSqGSIb3DQEJARYPdm1jYUB2bXdhcmUuY29tMIIBIjANBgkq</pre>	•
Cancel Cont	inue

- 9. Select Continue.
- 10. Select Install.
- 11. On the Cloud Control node, check the onboarded host **Details**.
- 12. Select **Certificate Invalid** and re-enter the host credentials.

Host Credentials will update to Valid.

Details

Туре	HostSystem
Trust Attestation Status 0	Unassessed
Virtual Machines	4
OS Version	VMware ESXi 7.0.3 build-19193900
External ID	HostSystem:host-22
IP Address	10.194. , fe80::9e7b:efff:
Host Credentials	✓ Valid
Global PIP	✓ Enabled (10.194. )
Proxy Access Ports	4
Proxy Access Ports Onboarded 0	4 ✔ Yes
Proxy Access Ports Onboarded <sup>①</sup> Sockets	4 ✔ Yes 1
Proxy Access Ports Onboarded <b>O</b> Sockets Trust Manifests	4 ✓ Yes 1 5

# Chapter 4. Additional resources and related products

- 4.1. CloudControl
- 4.2. Entrust products
- 4.3. nShield product documentation