# **Configure ISE SFTP with Certificate-based Authentication**

# Contents

Introduction Prerequisites Requirements Components Used Background Information Configure 1. Configure CentOS Server 2. Configure ISE Repository 3. Generate key pairs on the ISE server 3.1. ISE GUI 3.2. ISE CLI 4. Integration Verify Related Information

## Introduction

This document describes how to configure a Linux server with CentOS distribution as a Secure File Transfer Protocol (SFTP) server with Public Key Infrastructure (PKI) authentication towards Identity Services Engine (ISE).

# Prerequisites

### Requirements

Cisco recommends that you have knowledge of these topics:

- General ISE knowledge
- ISE repository configuration
- Basic Linux general knowledge

### **Components Used**

The information in this document is based on these software and hardware versions:

- ISE 2.2
- ISE 2.4
- ISE 2.6
- ISE 2.7

- ISE 3.0
- CentOS Linux release 8.2.2004 (Core)

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, please ensure that you understand the potential impact of any command.

### **Background Information**

To enforce security for file transfers, ISE can authenticate via PKI certificates through SFTP in order to ensure a more secure way to access repositories files.

# Configure

### 1. Configure CentOS Server

1.1 Create a directory as a root user.

```
mkdir -p /cisco/engineer
```

1.2. Create a user group.

groupadd tac

1.3. This command adds the user to the Main directory (files), it specifies the user belongs to the group **engineers.** 

```
useradd -d /cisco/engineer -s /sbin/nologin engineer
usermod -aG tac engineer
```

**Note**: The **/sbin/nologin** portion of the command indicates the user won't be able to log in through Secure Shell (SSH).

1.4. Proceed to create the directory to upload the files.

mkdir -p /cisco/engineer/repo
1.4.1 Set permissions for the directory files.

chown -R engineer:tac /cisco/engineer/repo
find /cisco/engineer/repo -type d -exec chmod 2775 {} \+
find /cisco/engineer/repo -type f -exec chmod 664 {} \+

1.5. Create the directory and the file in which the CentOS server performs the check for the certificates.

Directory:

```
mkdir /cisco/engineer/.ssh
chown engineer:engineer /cisco/engineer/.ssh
chmod 700 /cisco/engineer/.ssh
File:
```

touch /cisco/engineer/.ssh/authorized\_keys
chown engineer:engineer /cisco/engineer/.ssh/authorized\_keys
chmod 600 /cisco/engineer/.ssh/authorized\_keys
1.6. Create the login permissions in the sshd\_config system file.

In order to edit the file, you can use the vim Linux tool with this command.

vim /etc/ssh/sshd\_config
1.6.1 Add the specified lines below.

```
#Subsystem sftp /usr/libexec/openssh/sftp-server
Subsystem sftp internal-sftp
Match Group tac
ChrootDirectory %h
X11Forwarding no
AllowTCPForwarding no
ForceCommand internal-sftp
1.7. Run the command in order to verify the sshd_config system file syntaxis.
```

sshd -t

Note: No output means the syntax of the file is correct.

1.8. Proceed to restart the SSH service.

systemctl restart sshd

**Note**: Some Linux servers have **selinux** enforcement, to confirm this parameter, you can use the **getenforce** command. As a recommendation, if it is on **enforce** mode, change it to **permissive.** 

1.9. (optional) Edit the semanage.conf file to set the enforcement to permissive.

vim /etc/selinux/semanage.conf
Add the command setenforce0.

setenforce0

### 2. Configure ISE Repository

2.1. Proceed to add the repository through the ISE Graphic User Interface (GUI).

#### Navigate to Adminitration>System Maintenance>Repository>Add

-thick- Identity Services English	gine :	Home + Contact Vi	ability + Operations	+ Policy	<ul> <li>Administration</li> </ul>	Work Centers
System      Identity Mana;	perment >	Network Resources	Device Portal Managem	ent petGrid Se	rvices > Feed Ser	vice + Threat Centric NAC
Deployment Licensing	Certificates	s → Logging - Main	ienance Upgrade +	Backup & Resto	ore + Admin Accer	s → Settings
	0					
Patch Management		Repository List				
Repository	۲	too Luu L	fananta Kausalar - ( <b>b</b> . La	of a distance of	Vouse Costes	
Operational Data Purging		Con Two L	neverance well boars P. Dd	en guark key	North President	

2.2. Enter the proper configuration for your repository.

Repository List > Add Reposite	ory
Repository Configuration	on
* Repository Name	sftp_pki
* Protocol	SFTP •
Location	
* Server Name	10.88.240.102
* Path	1
Credentials	
* Enable PKI authentication	
* User Name	engineer
* Password	
Submit Cancel	

**Note**: If you need access to the repo directory instead of the root directory of engineer the target path needs to be /repo/.



### 3. Generate key pairs on the ISE server

#### 3.1. ISE GUI

Navigate to **Adminitration>System Maintenance>Repository>Generate key pairs**, as shown in the image.

**Note**: You must generate key pairs from the ISE GUI and Command Line Interface (CLI), in order to have full bidirectional access to the repository.

dealer Identity Services Engine	Home + C	Context Visibility	+ Operations + Policy	Administration      We	rit Centers
System → identity Management	Network Reso	urces > Device P	Portai Management peGri	Services > Feed Service	Threat Centric NAC
Deployment Licensing + Certification	ies > Logging	* Maintenance	Upgrade + Backup & R	store + Admin Access +	Settings
6	•				
Patch Management	Repositor	y List			
Repository G	100 4	Add L Canando K	in and The Depart wildle has	Vola Onla	
Operational Data Purging	Lear Lien Longare with base Richter brane with				

3.1.1. Enter a passphrase, this is required in order to protect the key pair.

Enter passphrase :	
•••••	
	Cancel U

Note: First generate the key pairs before the public keys are exported.

3.1.2. Proceed to export the Public key.

#### Navigate to Adminitration>System Maintenance>Repository>Export public key.

Select **Export public key**. A file is generated with the name **id\_rsa.pub** (ensure this is saved for future references).



#### 3.2. ISE CLI

3.2.1. Navigate to the CLI of the node in which you want to finish the configuration of the repository.

**Note**: From this point forward, the next steps are needed on each node that you would like to allow access to the SFTP repository with the use of the PKI authentication.

3.2.2. Run this command in order to add the IP of the Linux server to the **host\_key** system file.



3.2.3. Generate public CLI key.

```
crypto key generate rsa passphrase <passphrase>
ise24htts/admin# crypto key generate rsa passphrase admin123
```

3.2.4. Export the public key files from the CLI of ISE with this command.

crypto key export <name of the file> repository <repository name>

**Note**: You must have a previously accessible repository to which you can export the public key file.

ise24htts/admin# crypto key export public repository FTP

#### 4. Integration

4.1. Log in to your CentOS server.

Navigate to the folder in which you previously configured the **authorized\_key** file.

4.2. Edit the authorized key file.

Run the vim command in order to modify the file.

vim /cisco/engineer/.ssh/authorized\_keys

4.3. Copy and paste the content generated on steps 4 and 6 from the Generate key pairs section.

Public key generated from ISE GUI:

id\_rsa.pub
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQC1cgggs87651cBwTP16Grmf@r3MNx+ogorSuTmPToC+@zit161AbT1js/ PZreawf9urQXgQxEnSHaikf0FPA1rKqoLB1RGus2e1yNxVL06t1VFxBIEIEInQ799g9uRQ3XIDU1gC3q51fPsQp64rHsHmg0GbZ3L BMFvUgR3w0815X81y1yeLD116oL7RFq0LB1RGus2e1yNxVL06t1VFxBIEIENQ799g9uRQ3XIDU1gC3q51fPsQp64rHsHmg0GbZ3L ptP07B12vvIHN0hcZgG+Gnpw3U+SHxGMxs1fc393wCA4smzFnuNZ4/01jLppP4s2hqrAVedr+r90z+8XdsxY rootBise24htts
Public key generated from ISE CLI:
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQCaH+SANAYb47+NXFyuz06s0+gSykTRr6fdMryIiitCMBs0b6s5yc9S8VKpLyyocsIvc04/ vF/pSHoTE1R3wr2TL1vC1UrGnmgdQv4+@ynIbJ/f8EgZnXQ+fLKBoyLeVxPgd8cewL3HMV8g10HL12AdXt0B886tkmo40cmT/ HayXQ/a9YRZ1L2906pjKSWyuTkbUxWv9hx/ S55zp34pF790pq4UaTNX0yYuu328F6EFdKuFBSujAokP0nJTLN86dLAQ6x4kkkcXXXXKT8F1saPZwyJuqY8FNWtyiFIVY5Ct568zm D0Cj6vMav8L7G2dD14NZHr7LLpptgJFYAb6508\_admingise24htts Authorized\_key file on the Linux server:



4.4. After you paste the keys on the file, press ESC, proceed to run the **wq!** command in order to save the file.

# Verify

1. From the Linux server execute this command as root.

```
tail -f /var/log/secure
```

The output must be displayed, as shown in the image.

```
[[root@localhost -]# tail -f /var/log/secure
Apr 12 21:37:53 localhost sshd[668112]: Accepted publickey for root from 10.24.140.234 port 61159 ssh2: RSA SHA256:MNHNp2AtVXD8DbTswgPLKOGBaWFUue
GbKEW1EkcaeXU
Apr 12 21:37:53 localhost systemd[668112]: pam_unix(systemd-user:session): session opened for user root by (uid=0)
Apr 12 21:37:53 localhost sshd[668112]: pam_unix(sshd:session): session opened for user root by (uid=0)
Apr 12 21:38:27 localhost sshd[668208]: Accepted publickey for engineer from 10.24.140.234 port 61164 ssh2: RSA SHA256:MNHNp2AtVXD8DbTswgPLKD08aW
fUueObX[W1EkcaeXU
Apr 12 21:38:27 localhost systemd[668208]: pam_unix(systemd-user:session): session opened for user engineer by (uid=0)
Apr 12 21:38:27 localhost systemd[668208]: pam_unix(systemd-user:session): session opened for user engineer by (uid=0)
Apr 12 21:38:27 localhost sshd[668201]: pam_unix(sshd:session): session opened for user engineer by (uid=0)
Apr 12 21:38:27 localhost sshd[668201]: pam_unix(sshd:session): session opened for user engineer by (uid=0)
Apr 12 21:38:27 localhost sshd[668201]: pam_unix(sshd:session): session opened for user engineer by (uid=0)
Apr 12 21:38:27 localhost sshd[668201]: pam_unix(sshd:session): session opened for user engineer by (uid=0)
```

2. For ISE verification.

Navigate to Administration>System>Maintenance>Repository on the GUI.

Select the desired repository from the Repository List and select Validate.

deck Identity Services Engine	Home + Context Visibility + Ope	utors + Poley + Administration	+ Work Centers
System      Hidentity Management	Network Resources > Device Portal M	nagement perGrid Services > Feed Serv	ice > Threat Centric NAC
Deployment Licensing + Certificate	rs + Logging + Maintenance Upgra	de 🔸 Backup & Restore 🔸 Admin Access	<ul> <li>Settings</li> </ul>
0			
Patch Management	Repository List		
Repository 🕟	the last language and	Accession Marine Contra	
Operational Data Purging	/ EDK Add Generatz Kzy pars	Content public key Content providence	
	<ul> <li>Repository Name</li> </ul>	Protocol Host	Path
	C FTP	ftp 10.88.240.69	1
	UH-IONES10-BACKUPS	nfs ICNFS10-nfs.chp.clarian.	org /ISE_Backups
	backup	Rp 10.88.240.69	1
	□ sītp	sftp 10.88.240.69	1
	🗹 sftp_pki	sftp 10.88.240.102	1

You must see a pop-up which states the **Server Response** on the bottom right corner of the screen.



From the CLI, run the command **show repo sftp\_pki** in order to validate the keys.



In order to further debug ISE, execute this command on CLI:

debug transfer 7

The output must be displayed, as shown in the image:

Tarantitay aumining being transfer a
ise24htts/admin# show repo sftp_pki
6 [16745]:[info] transfer: cars_xfer.c[224] (admin): sftp dir of repository sftp_pki requested
6 [16745]:[inf0] transfer: cars_xfer_util.c[2208] [admin]: resolved server to 10.08.240.102
7 [16745]:[debug] transfer: sftp_handler.c[1027] [admin]: Running sftp command: 10.88.240.102 engineer +++ /repo/ ls -l /repo/
6 [16745]:[info] transfer: sftp_handler.c[554] [admin]: DEBUG: local user: admin UID: 0 sftp_run_parent FD: 5 remote host: 10.88.240.102 remote user: engineer comma
ndi la -l./repo/
7 [16747]:[debug] transfer: sftp_handler.c[268] [admin]: Executing SFTP command: 0 admin /usr/bin/sftp -oIdentityFile+/home/admin/.ssh/id_rsa -oUserKnownHostsFile+/
home/admin/.ssh/known_hosts -oPasswordAuthentication=no engineer010.88.240.102
7 (16745):[debug] transfer: sftp_handler.c[586] (admin): fd is:5
7 [16745]:[debug] transfer: sftp_handler.c(461] (admin): Found sftp prompt; No more data to read
7 [16745]:[debug] transfer: sftp_handler.c[917] [admin]: sftp_parent_status 0
7 (16745):[debug] transfer: cars_xfer_util.c(2315) [admin]: ssh_list xfer_succeeded
N Repository is empty

# **Related Information**

https://www.cisco.com/c/en/us/td/docs/security/ise/2-2/admin\_guide/b\_ise\_admin\_guide\_22/b\_ise\_admin\_guide\_22\_chapter\_01011.html