[Skip to end of metadata](https://wiki.ercot.com/pages/viewpage.action?pageId=141266235" \l "page-metadata-end)

* Created by [Williams, Gene](https://wiki.ercot.com/display/~fwilliams), last modified on [Jul 14, 2021](https://wiki.ercot.com/pages/diffpagesbyversion.action?pageId=141266235&selectedPageVersions=35&selectedPageVersions=36)

[Go to start of metadata](https://wiki.ercot.com/pages/viewpage.action?pageId=141266235#page-metadata-start)

Fresh **Install** and Initial Config of Twistlock ***Console***:

derived from <https://docs.twistlock.com/docs/compute_edition/install/install_openshift_4.html#create-an-openshift-project-for-prisma-cloud>

1. **Prep**

A. ssh [sysmgr@prtlccm0004.ercot.com](mailto:sysmgr@prtlccm0004.ercot.com)

B. cd ./twistlock

2. **Generate helm chart for Console:**

A. oc login api.<console's cluster>.[ercot.com](http://ercot.com/):6443

B. oc new-project twistlock  (if it errors saying twistlock already exists, that's ok)

C. oc project twistlock

D. twistcli console export openshift --storage-class "thin" --image-name "[docker-twistlock.edge.repo.ercot.com/twistlock/console:console\_21\_04\_412](http://docker-twistlock.edge.repo.ercot.com/twistlock/defender:defender_21_04_412)" --service-type "ClusterIP" --helm

3. **Installation and initial config:**

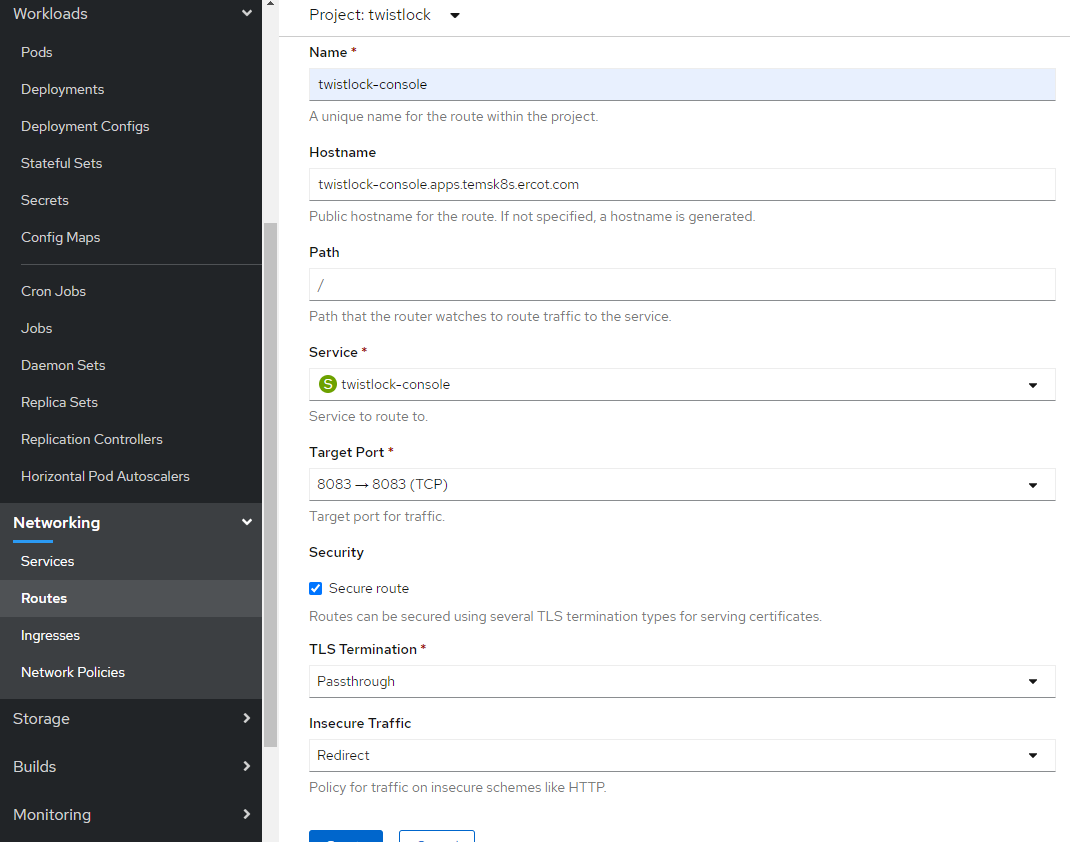
A.  tar -zxvf \*.gz

B. helm install -g ./twistlock-console -n twistlock

C. oc get pod   (Repeat every few seconds until pod status is "Running")

4.  Access to web UI:

A. Define route 'twistlock-console' in Openshift → Networking → Routes → "Create Route" button at top-right, and complete as shown here except change "temsk8s" to the cluster you are logged into:



B. Run this from teminal to remove namespace default network policy:  
     oc project twistlock && oc delete networkpolicy default-network-configuration

5. Login to Twistlock Console UI in browser:  [https://twistlock-console.apps.<cluster-name>.ercot.com/](https://twistlock-console.apps.temsk8s.ercot.com/#!/login)

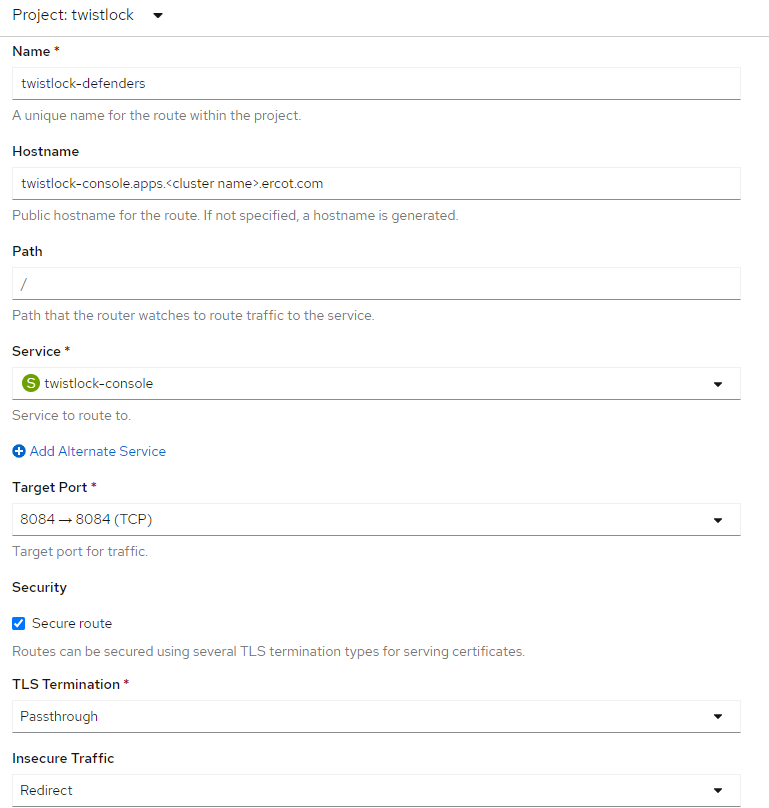
6. Enter admin for the username, and enter a password for you to store (this sets the initial local admin password) Note: Sometimes there is a matter of several seconds after submitting credentials and any activity in the Twistlock UI display with no progress or actuivity indicator in app or browser - this should never be more than 10 seconds.

7. You will be immediately prompted to enter the licence key.  Carefully paste it in without leading or trailing spaces, and submit.



8. Click the "Create Route" button again, and create the "twistlock-defenders" route, completing the form as shown here,

***except making the hostname twistlock-defenders.app.<cluster-name>..ercot.com:***



9. Add a SubjectAlternativeName to Console’s certificate to allow Defenders to establish a secure connection with Console like this:

i. oc get svc -n twistlock     (get Cluster IP of twistlock console)

ii. In Twistlock Console UI, Manage > Defenders > Names: add the internal IP from the previous command output and "[external-defenders.apps.](http://external-defenders.apps.temsk8s.ercot.com/)[<cluster-name>](https://twistlock-console.apps.temsk8s.ercot.com/#!/login)[.ercot.com](http://external-defenders.apps.temsk8s.ercot.com/)" as separate entries.  As soon as you add an entry, you'll be thrown back to the browser certificate warning, click back in, then wait on the white screen until the application graphic display returns.  (Note: Sometimes there is a matter of several seconds after submitting credentials and any activity in the Twistlock UI display with no progress or actuivity indicator in app or browser - this should never be more than 10 seconds)

Deploy Twistlock ***Defenders***:

1. **Generate helm chart for local defenders:**

A. oc login api.<console's cluster>.[ercot.com](http://ercot.com/):6443  
B. twistcli defender export openshift --address [https://twistlock-console.apps.](https://twistlock-console.apps.temsk8s.ercot.com/)[<cluster-name>](https://twistlock-console.apps.temsk8s.ercot.com/#!/login)[.ercot.com](https://twistlock-console.apps.temsk8s.ercot.com/) --cluster-address <Internal IP from cmd output in step 9.i.> --image-name [docker-twistlock.edge.repo.ercot.com/twistlock/defender:defender\_21\_04\_412](http://docker-twistlock.edge.repo.ercot.com/twistlock/defender:defender_21_04_412) --helm --cri  
    (When prompted, enter the admin password you set in step 6 above)

The command connects to Console’s API, specified in --address, to generate the Defender DaemonSet YAML config file or helm chart. The location where you run twistcli (inside or outside the cluster) dictates which Console address should be supplied.

The --cluster-address flag specifies the address Defender uses to connect to Console. For Defenders deployed inside the cluster, specify Prisma Cloud Console’s service name, twistlock-console or twistlock-console.twistlock.svc, or cluster IP address. For Defenders deployed outside the cluster, specify either Console’s external address, which is exposed by your external route.

2. **Installation and initial config:**

A. tar -zxvf \*.gz

B. helm install -g ./twistlock-defender -n twistlock

C. oc get pod   (Repeat until you see all defender pods in the state "Running")

D. Log into the Twistlock Console UI, and verify defender communication:    Manage > Defenders > Manage - Defenders should be displayed in main panel, and should show "Connected ..." in the "Status" column.

###  July 2021 above here ###############################################################################################

Twistlock Console **Patch/Upgrade** - Pre-deployment Steps

1. **Prep**

A. ssh [sysmgr@prtlccm0004.ercot.com](mailto:sysmgr@prtlccm0004.ercot.com)

B. cd ./twistlock/<version>/<site>         (example: cd ./twistlock/20.12/bastrop )

2. **Generate helm chart for Console:**

A. oc login api.<console's cluster>.[ercot.com](http://ercot.com/):6443                      (ex: oc login api.ebk8s.[ercot.com](http://ercot.com/):6443)

B. oc project twistlock

C. twistcli console export openshift --image-name "[docker-twistlock.repo.ercot.com/twistlock-console:<v](http://docker-ercot.repo.ercot.com/twistlock-console:20.12.531)ersion tag>" --service-type "ClusterIP" --helm

     (ex:  twistcli console export openshift --image-name "[docker-ercot.repo.ercot.com/twistlock-console:20.12.531](http://docker-ercot.repo.ercot.com/twistlock-console:20.12.531)" --service-type "ClusterIP" --helm)

3. **According to Twistlock documentation, there is a bug in helm that requires us to make a small edit in the Helm Chart that's generated:  *← disregard from 21.04 forward***

A. tar xvzf twistlock-console-helm.tar.gz

B. edit twistlock-console/templates/securitycontextconstraints.yaml, changing the value of 'apiVer' from 'v1' to '[security.openshift.io/v1](http://security.openshift.io/v1)'

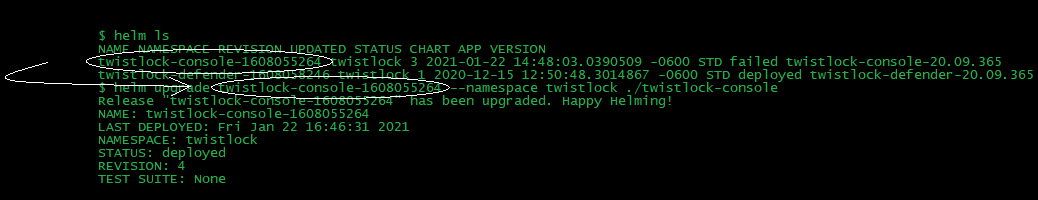
Twistlock Console **Patch/Upgrade** - Deployment Steps

4. **Installation and initial config:**

A. Get the helm *release* name of the twistlock console from '*helm ls*' output

B. helm upgrade <helm-release-name> --namespace twistlock ./twistlock-console

CLI should look something like this:



Twistlock **Patch/Upgrade** - Post-deployment Instructions

1. Log into Console to verify version and functionality.
2. Download Jenkins Plugin from Twistlock Console web UI under  *Manage > System > Downloads.*
3. Rename downloaded Jenkins Plugin to "twistlock-jenkins-plugin.hpi".
4. Push twistlock-jenkins-plugin.hpi to Prod JFrog Artifactory:  curl -T twistlock-jenkins-plugin.hpi [https://repo.ercot.com/artifactory/generic-thirdparty/twistlock-jenkins-plugin.hpi](https://repo.ercot.com/artifactory/generic-thirdparty/theplugin.hpiorwhateverextension)
5. Edit the defender pod yamls to reflect the correct image (with versions of twistlock that automatically update defender - this is being discontinued in future releases)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Twistlock Initial Config:

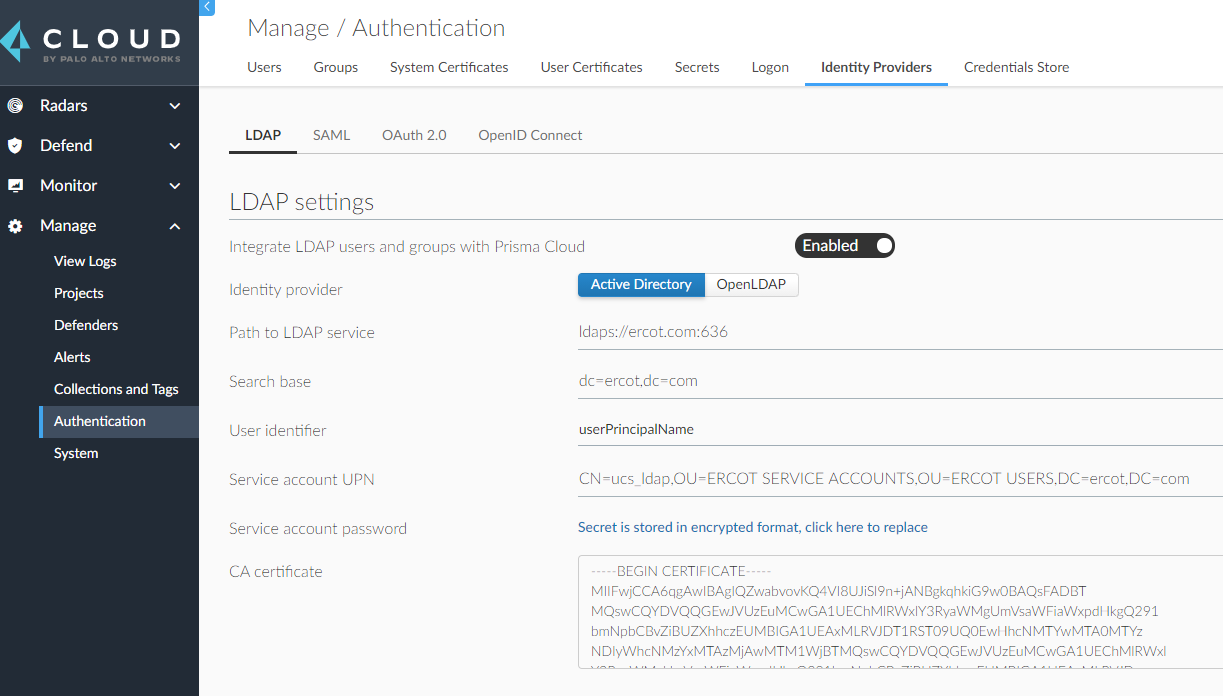
manage/authentication/ identity provider - enable ldap  
-----BEGIN CERTIFICATE-----  
MIIFwjCCA6qgAwIBAgIQZwabvovKQ4VI8UJiSl9n+jANBgkqhkiG9w0BAQsFADBT  
MQswCQYDVQQGEwJVUzEuMCwGA1UEChMlRWxlY3RyaWMgUmVsaWFiaWxpdHkgQ291  
bmNpbCBvZiBUZXhhczEUMBIGA1UEAxMLRVJDT1RST09UQ0EwHhcNMTYwMTA0MTYz  
NDIyWhcNMzYxMTAzMjAwMTM1WjBTMQswCQYDVQQGEwJVUzEuMCwGA1UEChMlRWxl  
Y3RyaWMgUmVsaWFiaWxpdHkgQ291bmNpbCBvZiBUZXhhczEUMBIGA1UEAxMLRVJD  
T1RST09UQ0EwggIiMA0GCSqGSIb3DQEBAQUAA4ICDwAwggIKAoICAQDkR0gbFioY  
ZNyZI7G7DPbXjIHajFUVborLViDUimU8tTa9D7hF8Zihg7wvb+aDYtXchurQu1wC  
7vteN3iv+0lyecpxALTgIHuXpJeZ+qKTrNvtWlj1H1tHCftcrQQJleODJka6xGBb  
9HLBM+gZRhZZ/cnYZMp9B0kEyJC0A1hI6wDxVwhfLZ4kfvs5BbeEsxTTD2wVZFC6  
XTEFmh/GF0kRQmfJTB0YPpLLh9IJdtkLiXc5iCkhmtfNfMecdqUhX+l1ORzpNLzS  
dGy777/yvtjOJPPz3gKKovLqXMHFToBC9kxL6IwLF0XPxlgkDOSvqHmIXbEBXXAM  
99DvtCBVUQVNyZRew6YX0/HNK6cD3vZk/qUKIY31Qbd2UVfQWIagjxaQ8dGmzmR3  
cPETdJHsYnAlxoGnXOsaBqaDfLA7umiB7BqKBLs+aUf/7g2muJaJglKYVTQOLa7C  
170r24VdYLo7OsoqkIN2F59oXnHwmXG06eLrZiTtbWZo9PE5BxyRcXSAkqVaOqmI  
J193yqya0vI7ZaFleRrNeszPP3oM8ndbRYkMdAgqecUEuouI4Ce1ktrNEGUmCjcB  
Vc0m7yeWh3N6XT580oAyMBKJuFeeee7mRJBaKc4SpPfcbECiWQUMx5D+hqXq9u2e  
8zbc4ZuTSyNU4Sp4nmExdJCSaSAGdjjKCQIDAQABo4GRMIGOMBMGCSsGAQQBgjcU  
AgQGHgQAQwBBMA4GA1UdDwEB/wQEAwIBhjAPBgNVHRMBAf8EBTADAQH/MB0GA1Ud  
DgQWBBRUYV/Km3Cf3zCUAKTIkPiKeOIkijASBgkrBgEEAYI3FQEEBQIDAQACMCMG  
CSsGAQQBgjcVAgQWBBR9aoWOIRwldu80xmiZEFgtiYKcczANBgkqhkiG9w0BAQsF  
AAOCAgEAAJM8thF/OtJb8LMfuFOjgVtJ5C2n3QvNRQ4Wk3U47jbmxnvqzuY+lMKh  
YJLnOX2Kq6EDJqS4EmxEGt2S1YeMID3d/C0LwddUgVYkvbW+oqr1yvbDCxgMEMF7  
jm22oHOUdk8elLosla3wILAzoHYRIoEiBwCc3gTQFAsiSSpJ+mdjBEyS9+74Qs+E  
SkBXGbc6B1y5sxNFi5Ih9tT2HYgU/hoEZiIu1OB7ezaZbu1Fhelve7RtdvpojuVN  
RttQgnvADgWr+viAaz7S+7Y2eQra+6zKO0IFgCF4BUX8LbszeBgxItk9aFNAUIEV  
Uit5HNqKAMXw4k17MBGijXm6H+NVD5Y4YaX5HyNXjJnHSzjSO/nxEyaGXunRipQ2  
dxNcaysoituj2KdKdxXJ3Pz/IGEmT4v3U+WyqEA7J6JpXfq83bSt04Mvhz3PBGj3  
wJCBoSnO4JB6wU1zxOLpHqqOYgLKcNMMGY43rE1SCan5SCQcOLV/89VuqThbhJAy  
sRahZuYNEXIx6De4aj1AJZd0A1MqqgzOJeKrSO3z1Thf7HK52NA/UbXG4GvqtcCn  
srRmXQvB9XnzIO1NDTTAxI/4HdGFdXQQM3azinihW+sC2YpcBRJpq8uhiWyFD4fx  
rH8uVQr5eCx305yea/YzajBVBE4fRNIneylgAxxLmgFWkMh2klo=  
-----END CERTIFICATE-----

Twistlock Initial Config and Integrations

1. Authentication

A. Identity Providers

    Fill the panel out as shown here and using the text values below the screenshot, being cautious not to include leading or trailing spaces:



i. Path to LDAP Service        <ldaps://ercot.com:636>

ii. Search base:                     dc=ercot,dc=com

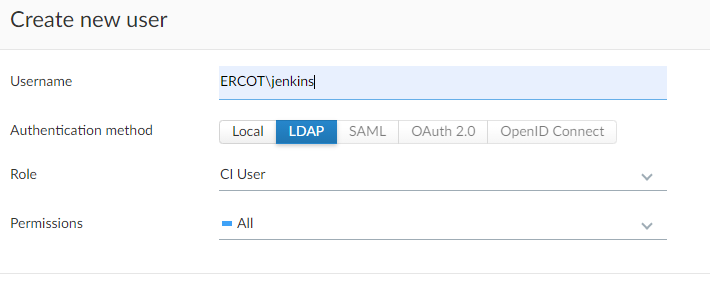
iii. Service account UPN       CN=ucs\_ldap,OU=ERCOT SERVICE ACCOUNTS,OU=ERCOT USERS,DC=ercot,DC=com

iv. Service account password:  <from vault>

v. CA Certificate: <from vault>

B. Users

    Add the users below the screenshot by clicking the "Add User" button on the "Users" tab, filling in the values as shown in the screenshot:

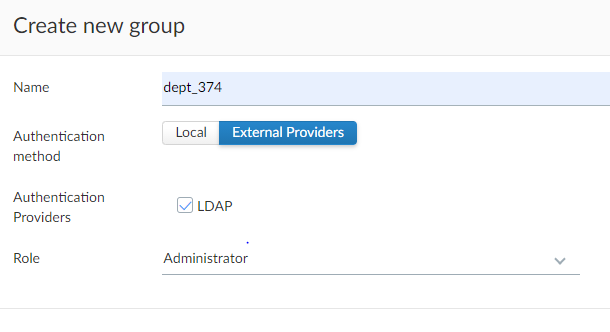


i. ERCOT\jenkins

ii. ERCOT\jenkinssvc

C. Groups

    Add the groups below the screenshot by clicking the "Add Group" button on the "Groups" tab, filling in the values as shown in the screenshot:



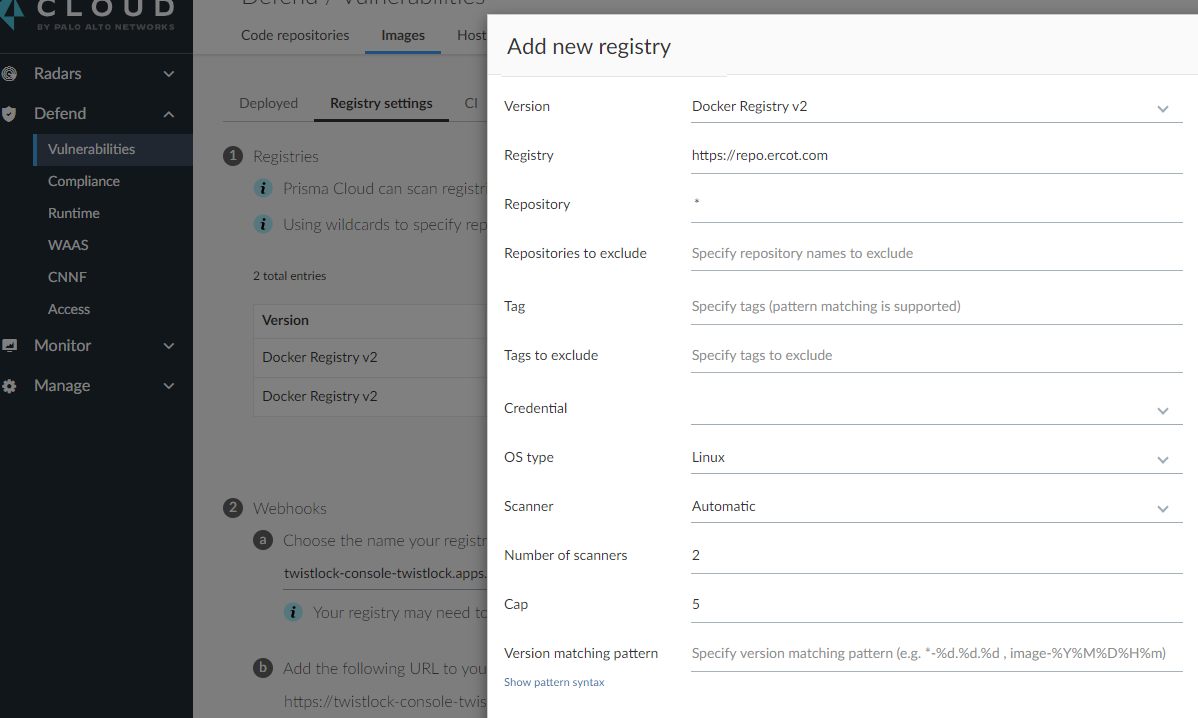
i. dept\_374

ii. dept\_370

2. Container Registry Scans

A. In the Twistlock Console UI, navigate to “Defend” > “Vulnerabilities”, click the “Registry settings” tab, and click the “Add Registry” button.

B. Complete the form as shown below



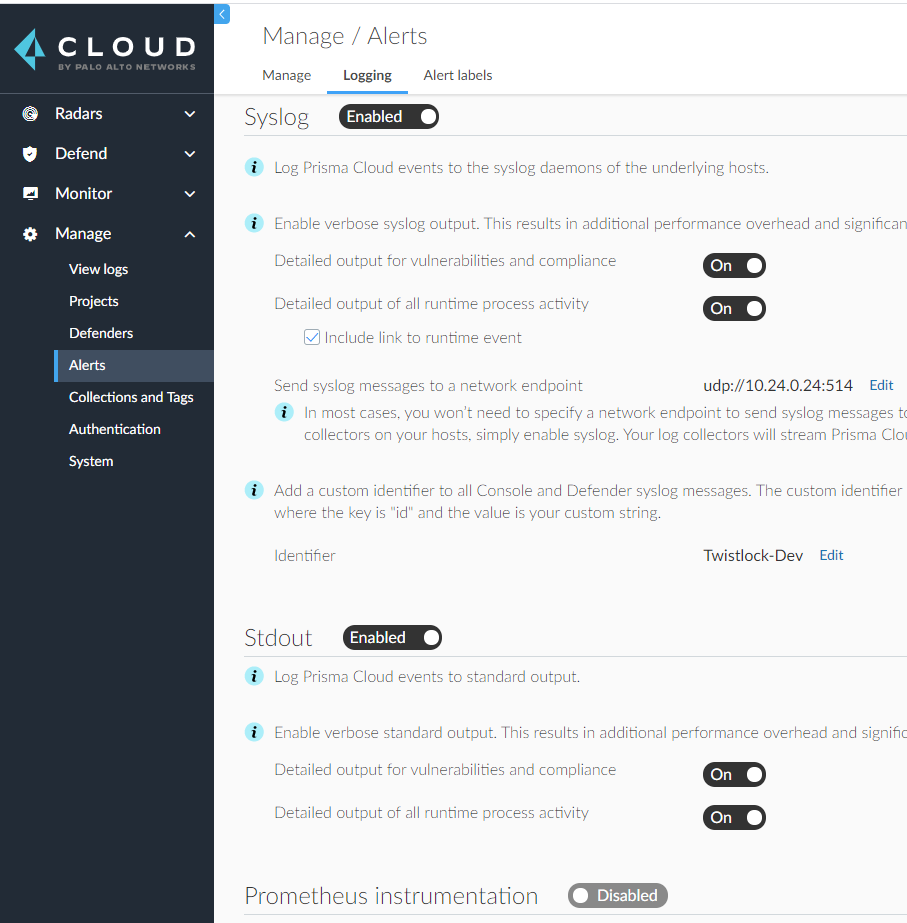
3. Splunk

A. In the Twistlock Console UI, navigate to “Manage” > “Alerts”, and select the “Logging” tab.

B. Complete the form as shown below,

      replacing “10.24.0.24 “ with [bas-log-syslog.ercot.com](http://bas-log-syslog.ercot.com/) for Prod Bastrop and [tay-log-syslog.ercot.com](http://tay-log-syslog.ercot.com/) for Prod Taylor in the “Send syslog messages to a network endpoint” field, and

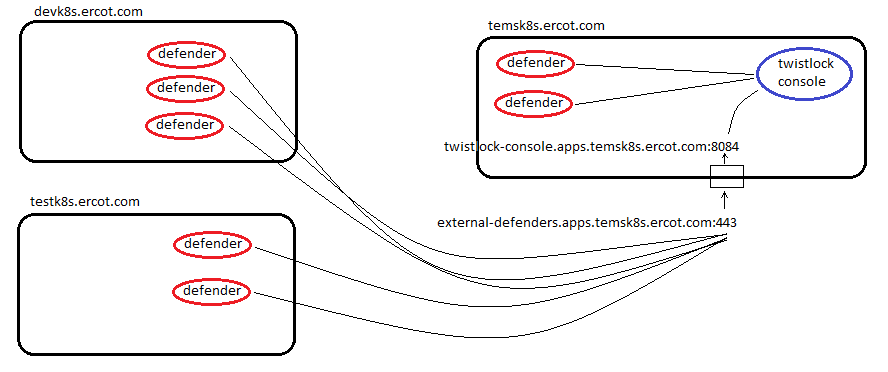
      replacing “–Dev” with “Prod-Bas” or “Prod-Tay” as appropriate in the “Identifier “ field.



##############################################################

**Defender-Console Relationships in Dev/Test/DNTS Environments**

Console: [temsk8s.ercot.com](http://temsk8s.ercot.com/)              Defenders: devk8s, testk8s, temsk8s



Install Remote Twistlock Defenders

1. define route external-defenders  
2. generate helm chart for remote defenders:  
oc login api.<remote defenders' cluster>.[ercot.com](http://ercot.com/):6443  
twistcli defender export openshift --address [https://twistlock-console.apps.](https://twistlock-console.apps.temsk8s.ercot.com/)[<cluster-name>](https://twistlock-console.apps.temsk8s.ercot.com/#!/login)[.ercot.com](https://twistlock-console.apps.temsk8s.ercot.com/) --cluster-address SAN\_defined\_in\_app <[external-defenders.apps.](http://external-defenders.apps.temsk8s.ercot.com/)[<cluster-name>](https://twistlock-console.apps.temsk8s.ercot.com/#!/login)[.ercot.com](http://external-defenders.apps.temsk8s.ercot.com/)> --image-name [dev-registry.ercot.com/twistlock/private:defender\_20\_09\_365](http://dev-registry.ercot.com/twistlock/private:defender_20_09_365) --helm --cri  
3. tar xvzf ?.tar.gz  
4. edit twistlock-defender/templates/securitycontextconstraints.yaml, changing apiVer: from 'v1' to '[security.openshift.io/v1](http://security.openshift.io/v1)'  ***← disregard from 21.04 forward***  
5. edit twistlock-defender/values.yaml, replacing the last line with:  
ws\_address: [wss://external-defenders.apps.](wss://external-defenders.apps.temsk8s.ercot.com/)[<cluster-name>](https://twistlock-console.apps.temsk8s.ercot.com/#!/login)[.ercot.com:443](wss://external-defenders.apps.temsk8s.ercot.com/)     ***← disregard from 21.04 forward***  
6. helm install -g ./twistlock-defender -n twistlock