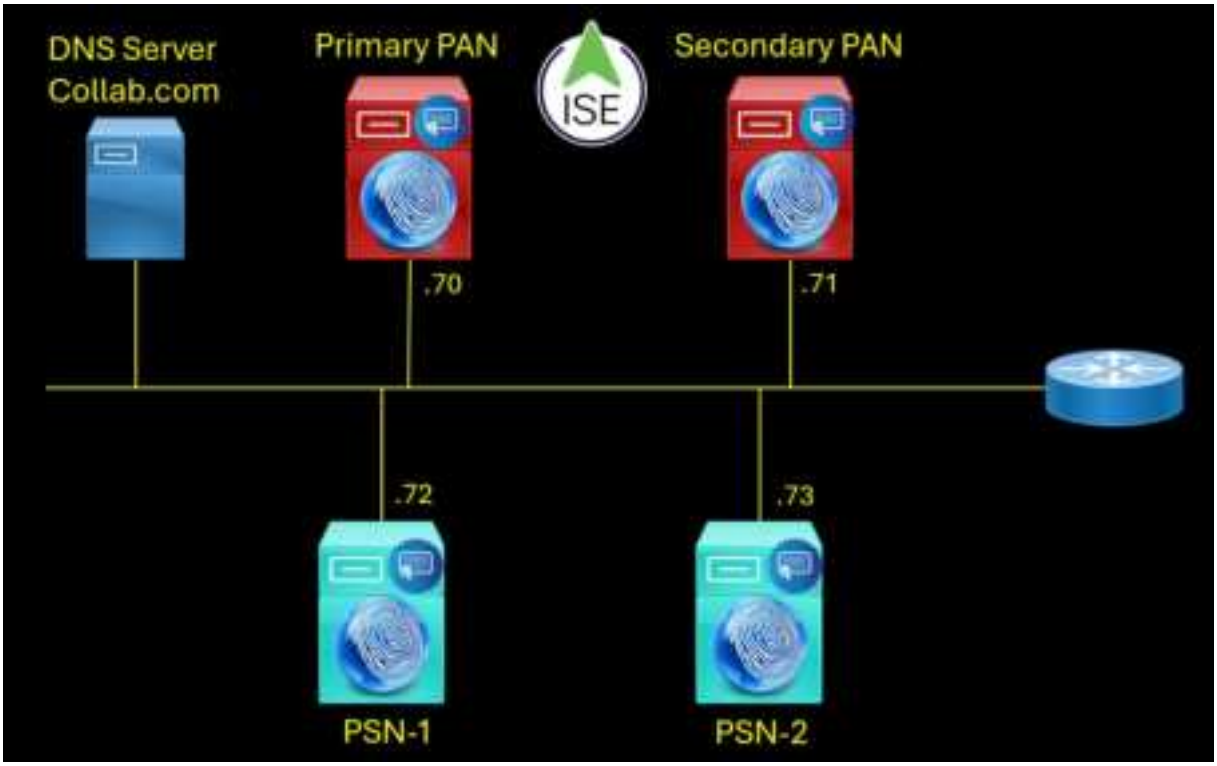
Demystifying PKI Infrastructure and Certificate Management With Cisco ISE Cluster Distributed Deployment



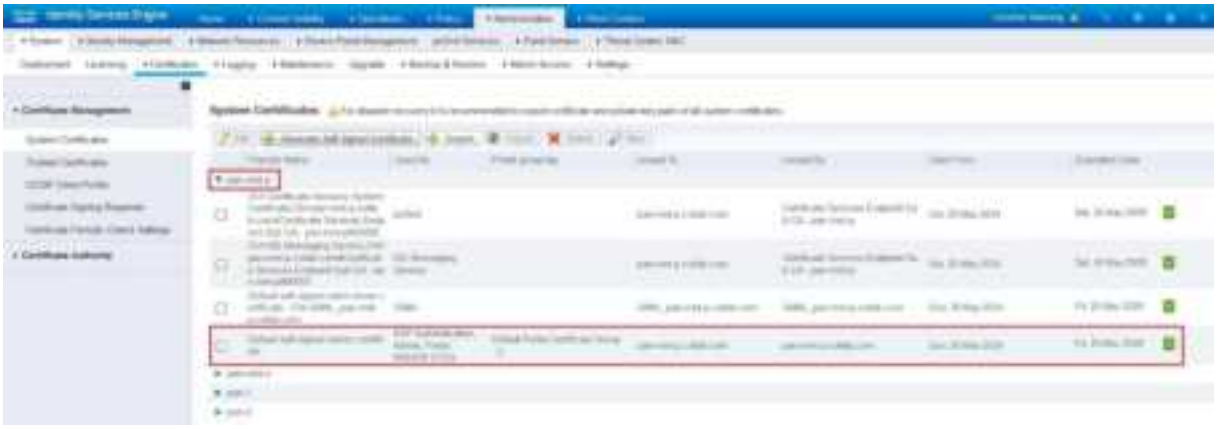
Redouane MEDDANE

In distributed deployment, each node installs a self-signed certificate signed by the system and has the Object Type : Certificate Authority. This certificate is unique in that it’s self-signed, essentially ensuring for its own authenticity. It doesn’t require validation from an external or superior entity because it already sits at the top of the trust hierarchy.

This self-signed certificate is used by the following services admin, EAP authentication, RADIUS DTLS and portals.

Below the list of the self-signed certificate used by each node. Each certificate has the Common Name equal to the FQDN of the node.

PAN-MNT-P.




Certificat
Général
Détails
Chemin d'accès de certification
Chemin d'accès de certification
pan-mnt-p.collab.com
Afficher le certificat
État du certificat :
Ce certificat racine de l'autorité de certification n'est pas de confiance car il ne fait pas partie du magasin d'autorités de certification de racine de confiance.

PAN-MNT-S.


Certificat
Général
Détails
Chemin d'accès de certification
Informations sur le certificat
Vous ne pouvez pas faire confiance à ce certificat racine de l'autorité de certification. Pour activer la confiance, installez ce certificat dans le magasin d'autorités de certification de la racine de confiance.
Délivré à : pan-mnt-s.collab.com
Délivré par pan-mnt-s.collab.com
Valide du 26/05/2024 au 25/05/2029
Installer un certificat...
Déclaration de l'émetteur


Certificat
Général
Détails
Chemin d'accès de certification
Chemin d'accès de certification
pan-mnt-s.collab.com
Afficher le certificat
État du certificat :
Ce certificat racine de l'autorité de certification n'est pas de confiance car il ne fait pas partie du magasin d'autorités de certification de racine de confiance.

PSN-1.


Certificat
Général
Détails
Chemin d'accès de certification
Informations sur le certificat
Vous ne pouvez pas faire confiance à ce certificat racine de l'autorité de certification. Pour activer la confiance, installez ce certificat dans le magasin d'autorités de certification de la racine de confiance.
Délivré à : psn-1.collab.com
Délivré par psn-1.collab.com
Valide du 26/05/2024 au 25/05/2029
Installer un certificat...
Déclaration de l'émetteur


Certificat
Général
Détails
Chemin d'accès de certification
Chemin d'accès de certification
psn-1.collab.com
Afficher le certificat
État du certificat :
Ce certificat racine de l'autorité de certification n'est pas de confiance car il ne fait pas partie du magasin d'autorités de certification de racine de confiance.

PSN-2.

When you install Cisco ISE cluster, an internal PKI hierarchy is built. The certificate management are centralized on the Primary PAN where you can create, delete and renew the nodes certificates.

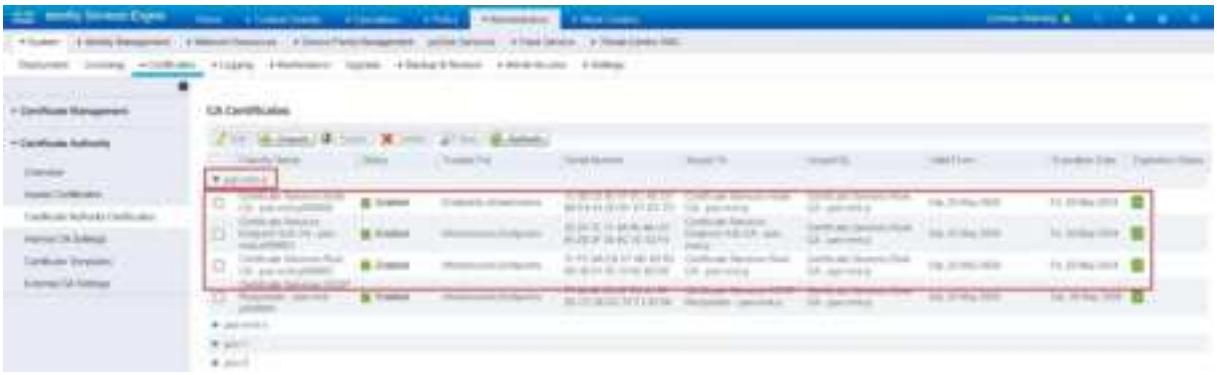
First the primary PAN has the Root CA certificate representing the top of trust hierarchy as shown below.

The PAN has also a subordinate certificate called Certificate Services Nodes CA - pan-mnt-p signed by its Root CA certificate as shown below.

In additon the Primary PAN generates a subordinate certificate called Certificate Services Endpoint Sub CA – pan-mnt-p and it is signed by the Node Certificate of the primary PAN called "Certificate Services Nodes CA - pan-mnt-p".


Certificat
Général
Détails
Chemin d'accès de certification
Informations sur le certificat
Impossible de vérifier ce certificat auprès d'une Autorité de certification de confiance.
Délivré à : Certificate Services Endpoint Sub CA - pan-mnt-p
Délivré par Certificate Services Node CA - pan-mnt-p
Valide du 25/05/2024 au 26/05/2034
Installer un certificat...
Déclaration de l'émetteur


Certificat
Général
Détails
Chemin d'accès de certification
Chemin d'accès de certification
Certificate Services Root CA - pan-mnt-p
Certificate Services Node CA - pan-mnt-p
Certificate Services Endpoint Sub CA - pan-mnt-p
Afficher le certificat
État du certificat :
Ce certificat est valide.



When you register the secondary PAN two subordinate certificates are generated.

Certificate Services Nodes CA - pan-mnt-s signed by the primary PAN Root CA.

Certificate Services Endpoint Sub CA - pan-mnt-s signed by the subordinate certificate Services Nodes CA - pan-mnt-s.

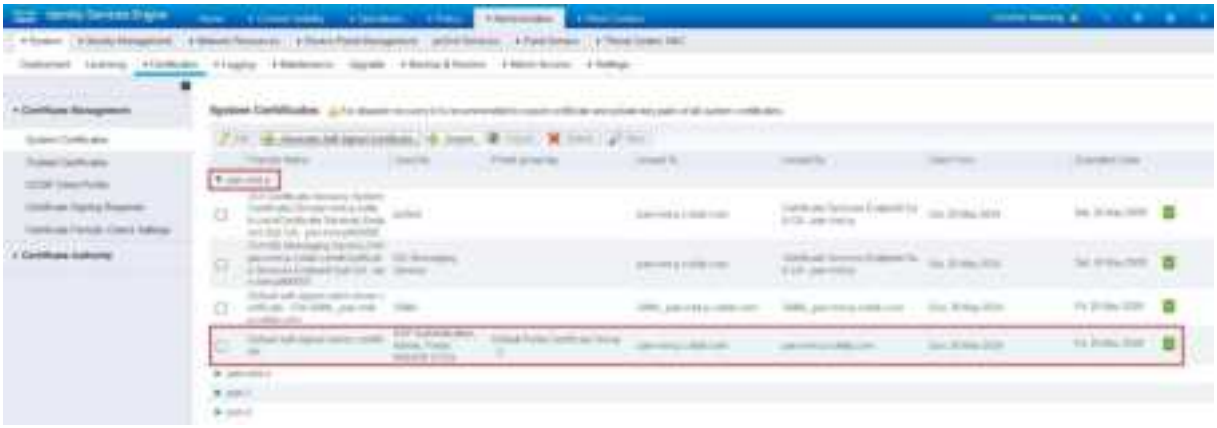
In addition, a server or entity certificate is generated for the secondary PAN with the Common Name equal to the FQDN pan-mnt-s.collab.com, this server certificate is signed by the subordinate certificate Services Endpoint Sub CA - pan-mnt-s.collab.com.

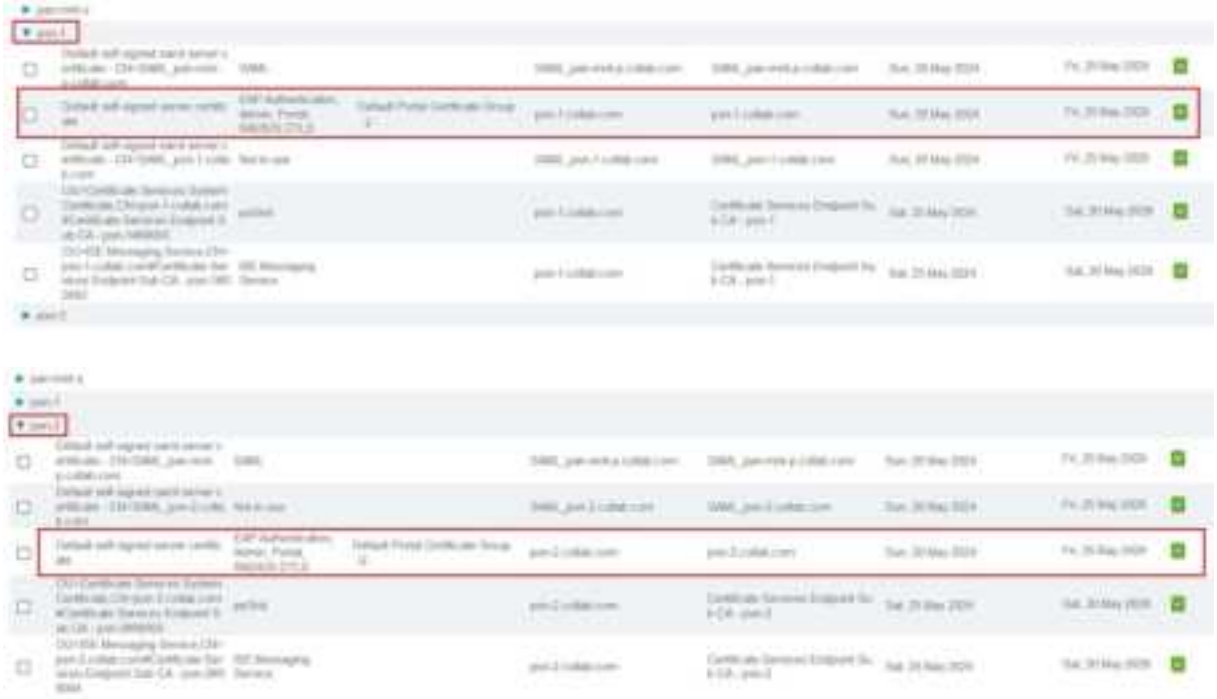
When you register the Policy Service Node PSN, each PSN node is provisioned a subordinate certificate called Certificate Services Endpoint Sub CA and it is signed by the Node Certificate of the primary PAN called "Certificate Services Nodes CA - pan-mnt-p".

In this example, the PSN-1 is provisioned with a subordinate certificate called "Certificate Services Endpoint Sub CA - PSN-1".

The PSN-2 is provisioned with a subordinate certificate called "Certificate Services Endpoint Sub CA - PSN-2".

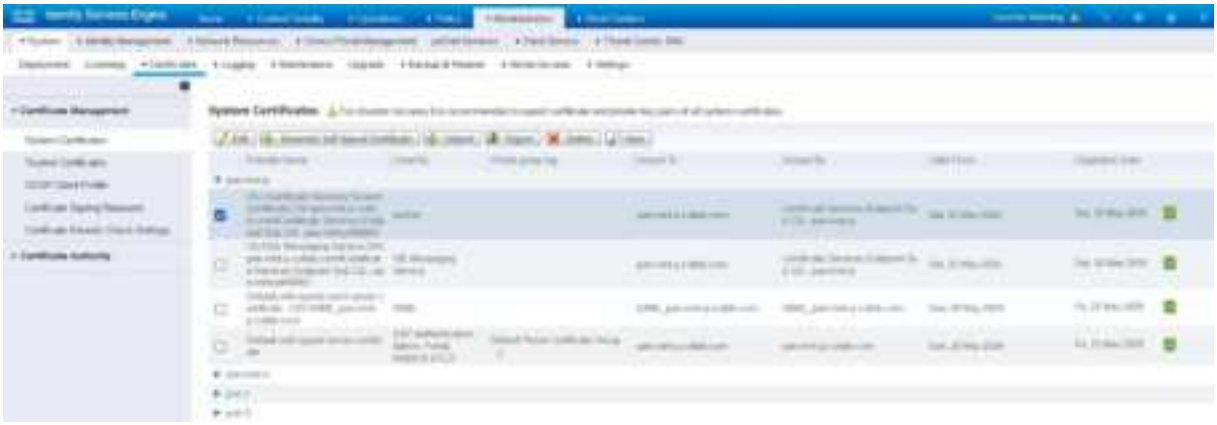
By default, each node uses the self-signed certificate for the following services: admin access, EAP authentication, RADIUS DTLS and portals.

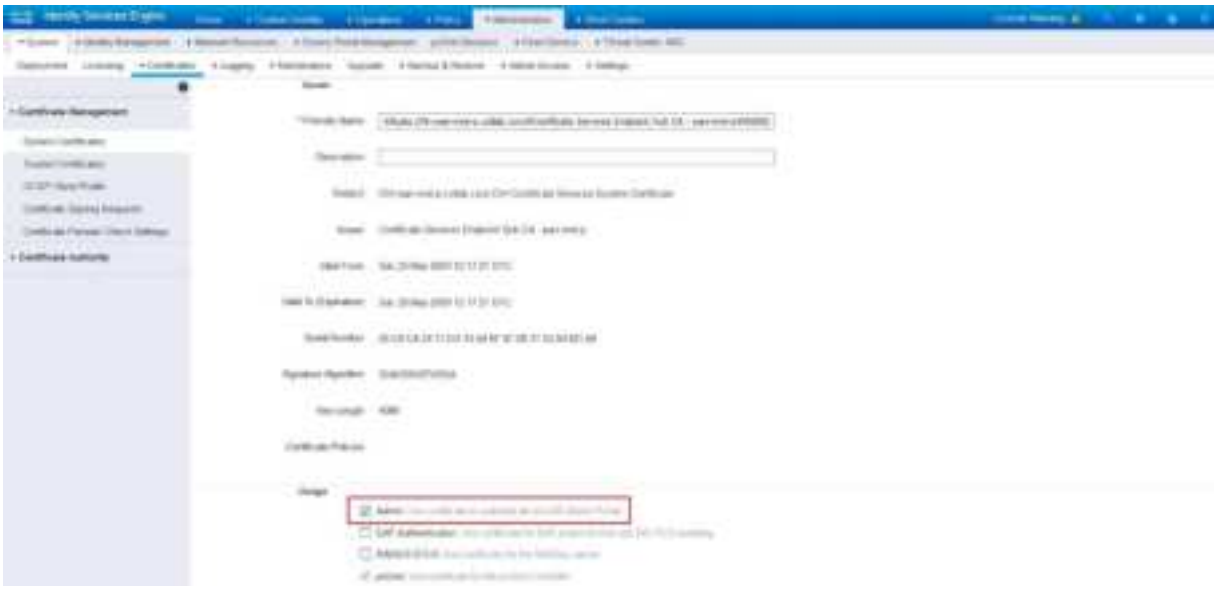




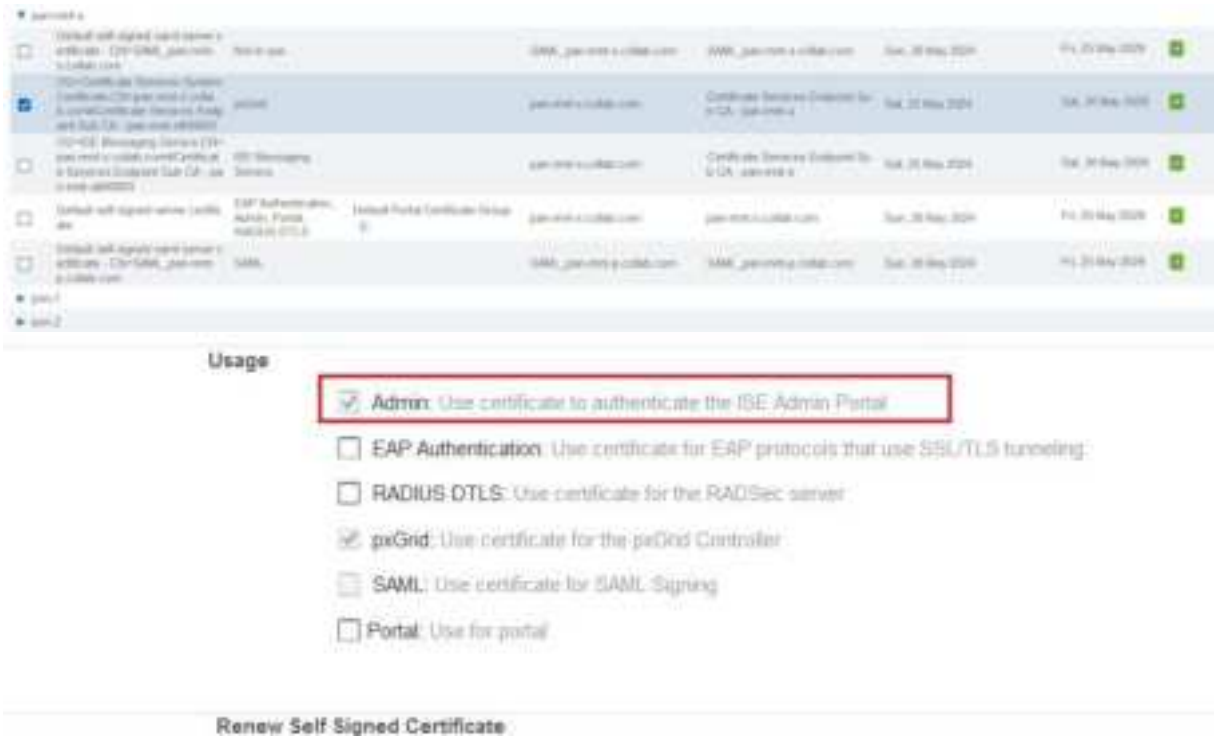
We can instruct each node to use another system certificate such as the one used for pxGrid which is signed by the Certificate Services Endpoint Sub CA of each node.

Primary PAN pan-mnt-p.

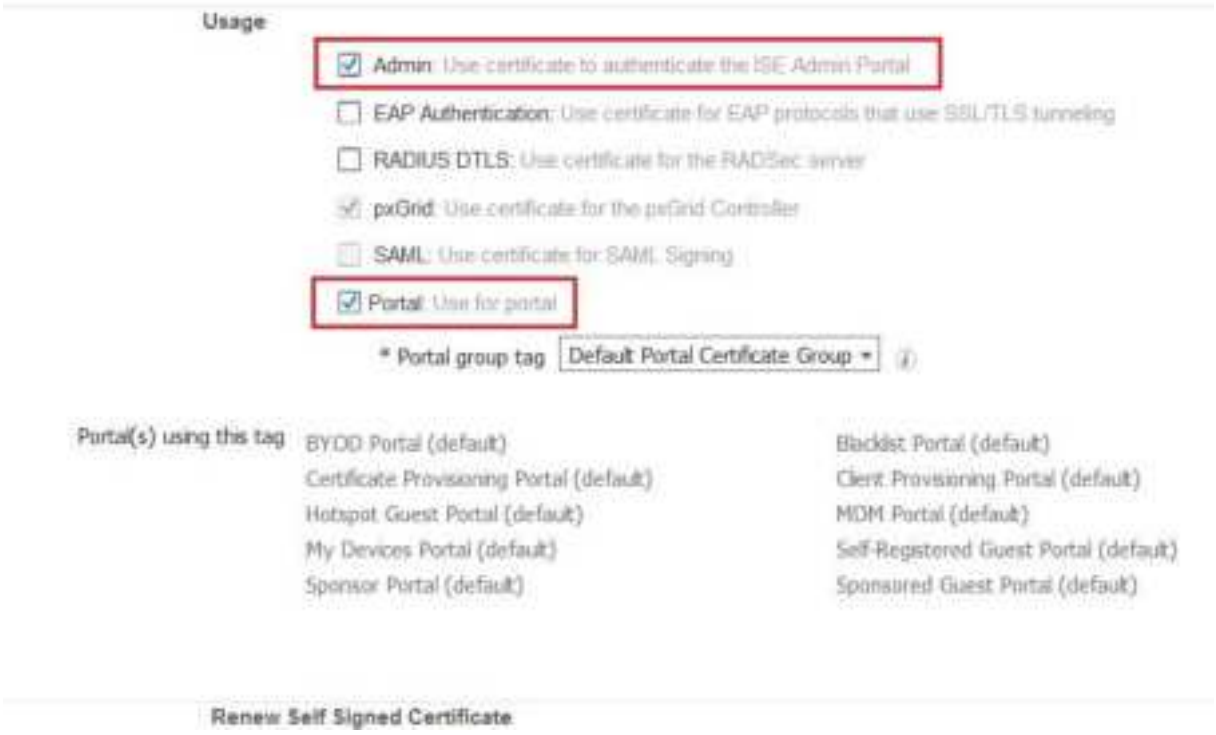




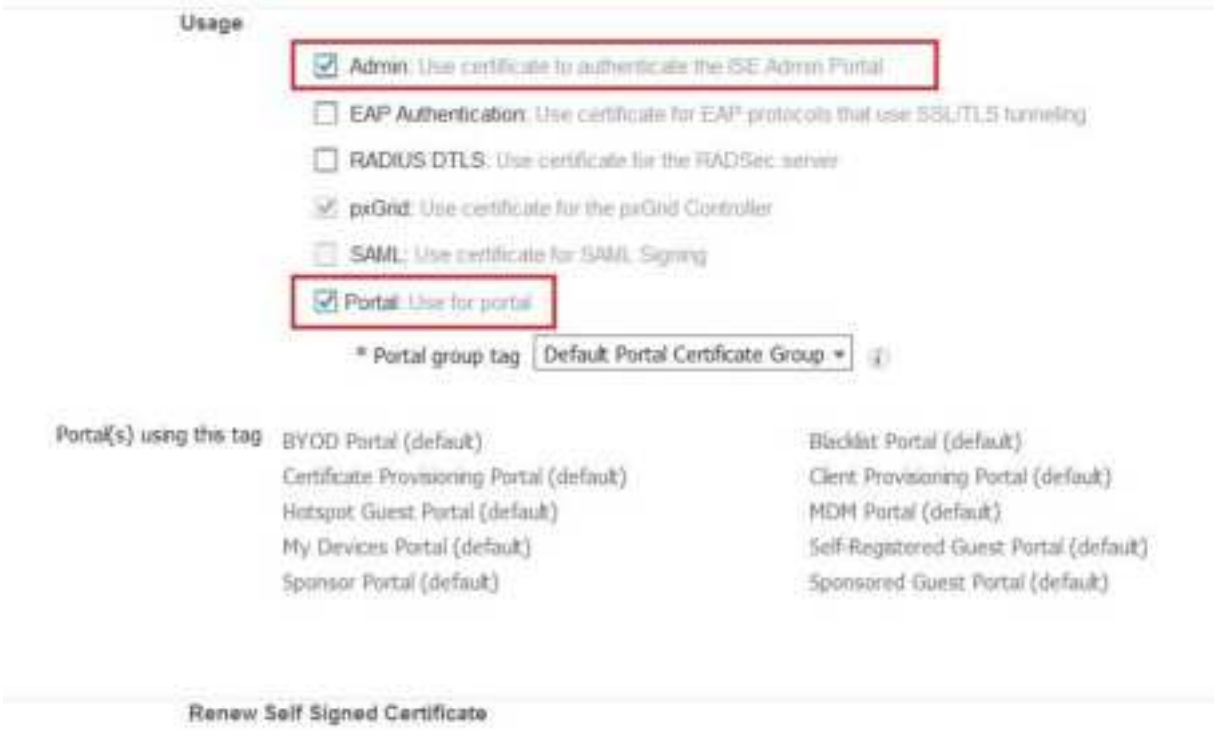
Secondary PAN pan-mnt-s.



Policy Service Node PSN-1.



Policy Service Node PSN-2.



The primary PAN is now using the system certificate for admin access and signed by its own subordinate CA certificate called Certificate Services Endpoint Sub CA – pan-mnt-p.

The secondary PAN is now using the system certificate for admin access and signed by its own subordinate CA certificate called Certificate Services Endpoint Sub CA – pan-mnt-s.

The Policy Service Node PSN-1 is now using the system certificate for admin access/portals and signed by its own subordinate CA certificate called Certificate Services Endpoint Sub CA – psn-1.

The Policy Service Node PSN-2 is now using the system certificate for admin access/portals and signed by its own subordinate CA certificate called Certificate Services Endpoint Sub CA – psn-2.


Certificat
psn-2.collab.com
Certificate Services Endpoint Sub CA - psn-2
Certificate Services Node CA - pan-mnt-p
Certificate Services Root CA - pan-mnt-p
Nom du sujet
Unité organisationnelle Certificate Services System Certificate
Nom courant psn-2.collab.com
Nom de l'émetteur
Nom courant Certificate Services Endpoint Sub CA - psn-2