Client Provisioning Policy

Define the Client Provisioning Policy to determine what users will receive upon login and user session initiation:
For Agent Configuration: version of agent, agent profile, agent compliance module, and/or agent customization package.
For Native Supplicant Configuration: wizard profile and/or wizard. Drag and drop rules to change the order.

	Rule Name		Identity Groups		Operating Systems		Other Conditions		Results
☑	IOS	If	Any	and	Apple iOS All	and	Condition(s)	then	TDHB NSP Profile

Dictionaries ▸ Conditions ▾ Results

- ▸ Authentication
- ▸ Authorization
- ▸ Profiling
- ▸ Posture
- ▾ Client Provisioning
  - Resources

Resources

Edit | Add ▾ | Duplicate | Delete

	Name	Type	Version	Last Update	Description
	tdhbl				
☐	TDHB NSP Profile	Native Supplicant Profile	Not Applicable	2020/03/03 13:23:50	

Policy Sets | Profiling | Posture | Client Provisioning | ▾ Policy Elements

Dictionaries ▸ Conditions ▾ Results

- ▸ Authentication
- ▸ Authorization
- ▸ Profiling
- ▸ Posture
- ▾ Client Provisioning
  - Resources

Native Supplicant Profile > TDHB NSP Profile

Native Supplicant Profile

Name * TDHB NSP Profile

Description

Operating System * ALL

Wireless Profile(s)

Multiple SSIDs can be configured, and the first profile will b… t profiles).
Proxy Auto-Config File URL will be used for automatic conf…
If no Proxy Auto-Config File URL is defined then the Proxy …

Edit | Add | Duplicate | Delete

	SSID Name	Proxy Auto-Config File …	P…
☑	TDHB-BYOD-2		

Wireless Profile

SSID Name * TDHB-BYOD-2

Proxy Auto-Config File URL

Proxy Host/IP

Proxy Port

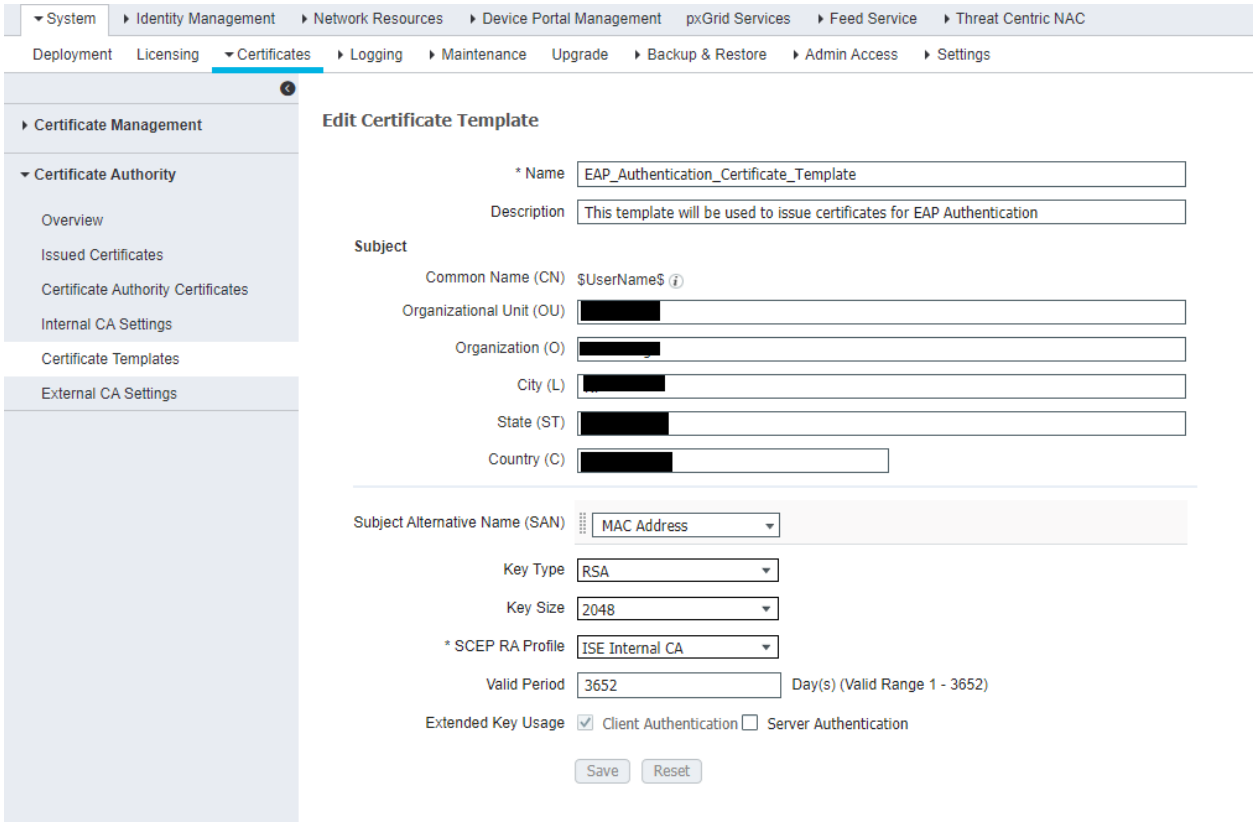
Security * WPA2 Enterprise

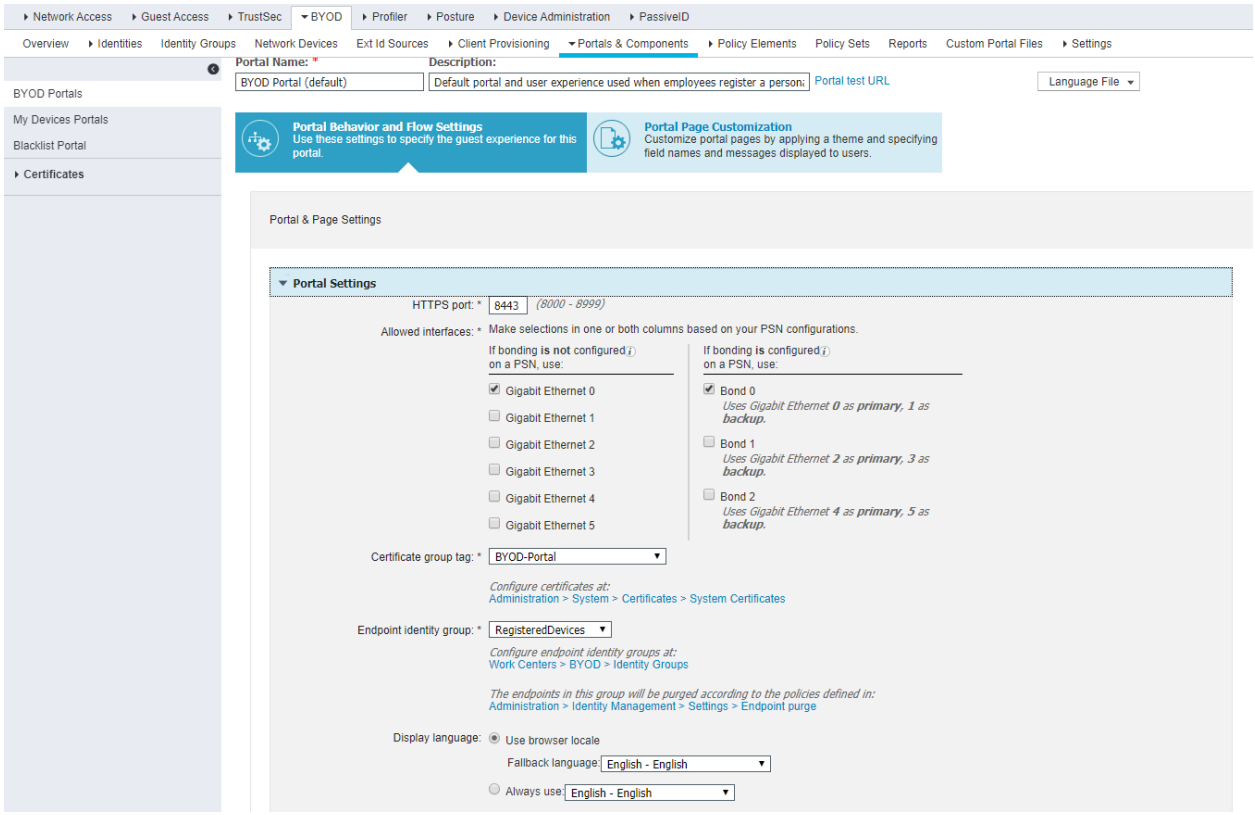
Allowed Protocol * TLS

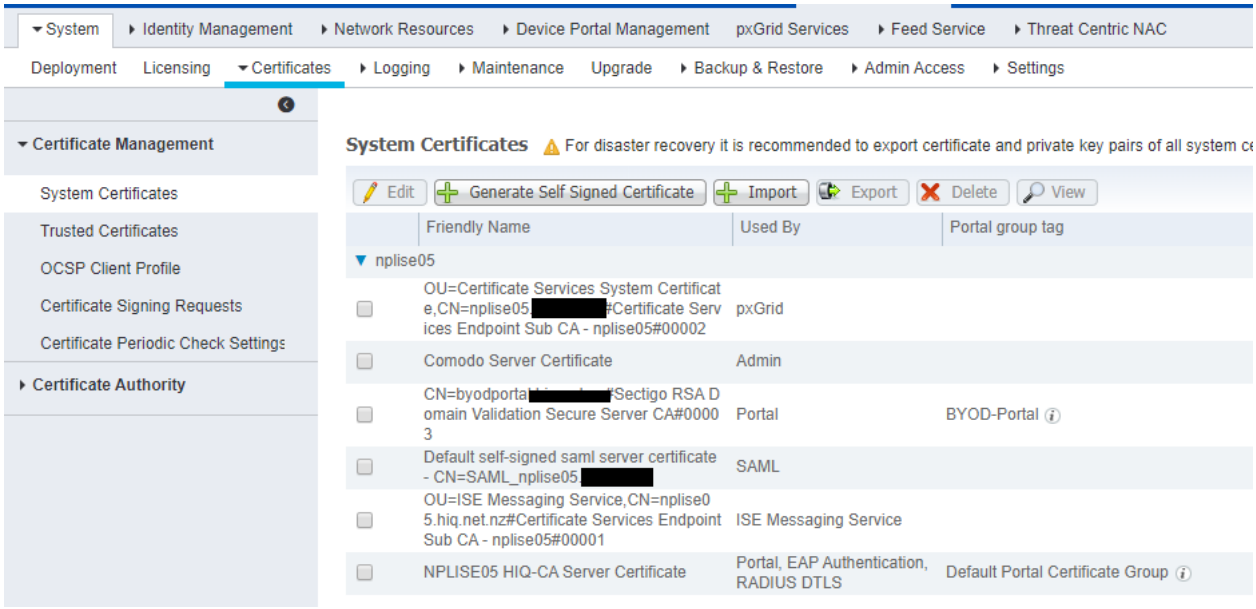
Certificate Template EAP_Authentication_Certificate_Template

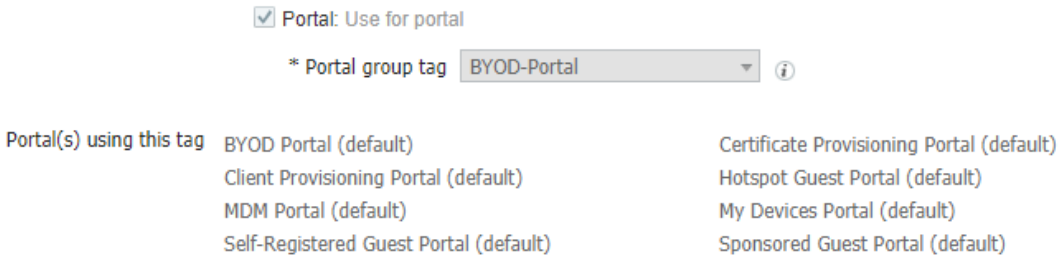
▸ Optional Settings

Submit | Cancel


System
Identity Management
Network Resources
Device Portal Management
pxGrid Services
Feed Service
Threat Centric NAC
Deployment
Licensing
Certificates
Logging
Maintenance
Upgrade
Backup & Restore
Admin Access
Settings
Certificate Management
Certificate Authority
Overview
Issued Certificates
Certificate Authority Certificates
Internal CA Settings
Certificate Templates
External CA Settings
Edit Certificate Template
* Name
EAP_Authentication_Certificate_Template
Description
This template will be used to issue certificates for EAP Authentication
Subject
Common Name (CN)
$UserName$
Organizational Unit (OU)
Organization (O)
City (L)
State (ST)
Country (C)
Subject Alternative Name (SAN)
MAC Address
Key Type
RSA
Key Size
2048
* SCEP RA Profile
ISE Internal CA
Valid Period
3652
Day(s) (Valid Range 1 - 3652)
Extended Key Usage
Client Authentication
Server Authentication
Save
Reset


Network Access
Guest Access
TrustSec
BYOD
Profiler
Posture
Device Administration
PassiveID
Overview
Identities
Identity Groups
Network Devices
Ext Id Sources
Client Provisioning
Portals & Components
Policy Elements
Policy Sets
Reports
Custom Portal Files
Settings
BYOD Portals
My Devices Portals
Blacklist Portal
Certificates
Portal Name: *
BYOD Portal (default)
Description:
Default portal and user experience used when employees register a person:
Portal test URL
Language File
Portal Behavior and Flow Settings
Use these settings to specify the guest experience for this portal.
Portal Page Customization
Customize portal pages by applying a theme and specifying field names and messages displayed to users.
Portal & Page Settings
Portal Settings
HTTPS port: *
8443
(8000 - 8999)
Allowed interfaces: *
Make selections in one or both columns based on your PSN configurations.
If bonding is not configured on a PSN, use:
Gigabit Ethernet 0
Gigabit Ethernet 1
Gigabit Ethernet 2
Gigabit Ethernet 3
Gigabit Ethernet 4
Gigabit Ethernet 5
If bonding is configured on a PSN, use:
Bond 0
Uses Gigabit Ethernet 0 as primary, 1 as backup.
Bond 1
Uses Gigabit Ethernet 2 as primary, 3 as backup.
Bond 2
Uses Gigabit Ethernet 4 as primary, 5 as backup.
Certificate group tag: *
BYOD-Portal
Configure certificates at:
Administration > System > Certificates > System Certificates
Endpoint identity group: *
RegisteredDevices
Configure endpoint identity groups at:
Work Centers > BYOD > Identity Groups
The endpoints in this group will be purged according to the policies defined in:
Administration > Identity Management > Settings > Endpoint purge
Display language:
Use browser locale
Fallback language:
English - English
Always use:
English - English


System
Identity Management
Network Resources
Device Portal Management
pxGrid Services
Feed Service
Threat Centric NAC
Deployment
Licensing
Certificates
Logging
Maintenance
Upgrade
Backup & Restore
Admin Access
Settings
Certificate Management
System Certificates
Trusted Certificates
OCSP Client Profile
Certificate Signing Requests
Certificate Periodic Check Settings
Certificate Authority
System Certificates
For disaster recovery it is recommended to export certificate and private key pairs of all system ce
Edit
Generate Self Signed Certificate
Import
Export
Delete
View
Friendly Name
Used By
Portal group tag
nplise05
OU=Certificate Services System Certificate,CN=nplise05[redacted]#Certificate Services Endpoint Sub CA - nplise05#00002
pxGrid
Comodo Server Certificate
Admin
CN=byodporta[redacted]#Sectigo RSA Domain Validation Secure Server CA#00003
Portal
BYOD-Portal
Default self-signed saml server certificate - CN=SAML_nplise05.[redacted]
SAML
OU=ISE Messaging Service,CN=nplise05.hiq.net.nz#Certificate Services Endpoint Sub CA - nplise05#00001
ISE Messaging Service
NPLISE05 HIQ-CA Server Certificate
Portal, EAP Authentication, RADIUS DTLS
Default Portal Certificate Group


Portal: Use for portal
* Portal group tag
BYOD-Portal
Portal(s) using this tag
BYOD Portal (default)
Client Provisioning Portal (default)
MDM Portal (default)
Self-Registered Guest Portal (default)
Certificate Provisioning Portal (default)
Hotspot Guest Portal (default)
My Devices Portal (default)
Sponsored Guest Portal (default)