

# Prepare the Infrastructure

---



**Richard Hicks**

Richard M. Hicks Consulting, Inc.

@richardhicks    [www.richardhicks.com](http://www.richardhicks.com)



# Overview



## Prepare the Infrastructure

### Overview

- Active Directory security groups
- Certificate templates
- Auto-enrollment



# Security Groups

---



# Active Directory Security Groups

**VPN Servers**

**NPS Servers**

**VPN Users**

**VPN Devices**



# Security Group Application



## Certificate Enrollment

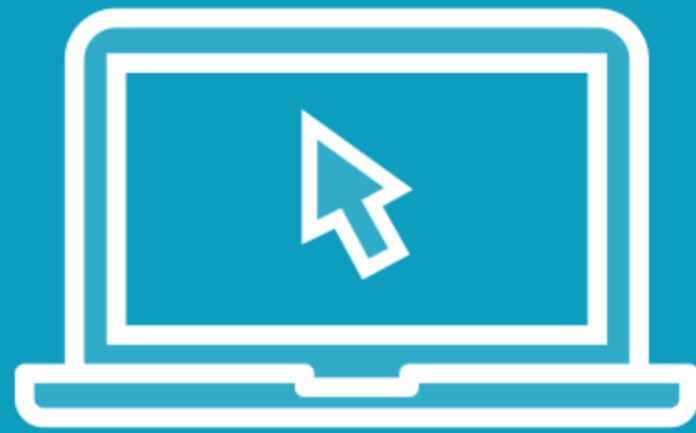
**Restrict certificate enrollment to specific users or devices**



## VPN Access

**Control which users can access the VPN**

# Demo



## Active Directory Security Groups

Create global security groups using...

- UI
- PowerShell



# Certificate Templates

---



# Certificate Templates

**VPN Servers**

**NPS Servers**

**VPN Users**

**VPN Devices**

**Domain Controllers**





# VPN Server Certificate Template

---



# VPN Server Certificate Template



**Machine certificate**



**Required EKUs: Server Authentication, IP security IKE Intermediate**



**Subject name must be supplied in the request!**



The subject of the VPN server certificate must include the public hostname.



Demo



## VPN Server Certificate Template



# NPS Server Certificate Template

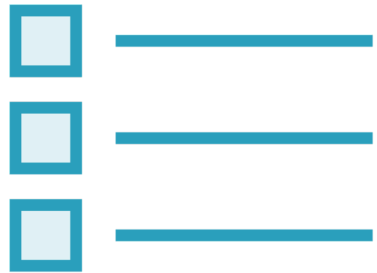
---



# NPS Server Certificate Template



**Machine certificate**



**Required EKUs: Server Authentication**



**Subject name is the server hostname**



Demo



## NPS Server Certificate Template



# User Certificate Template

---

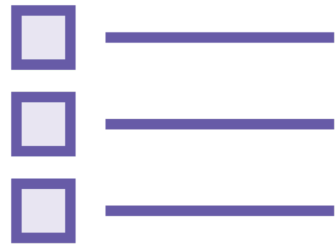




# VPN User Certificate Template



**User certificate**



**Required EKUs: Client Authentication**



**Subject name is the user's common name**



**Subject alternative name is the user's UPN**



**Enroll to TPM**



TPM: Hardware-based  
cryptography processor with  
advanced security features.



# Demo



## User Certificate Template



# Device Certificate Template

---



# VPN Device Certificate Template



**Machine certificate**



**Required EKUs: Client Authentication**



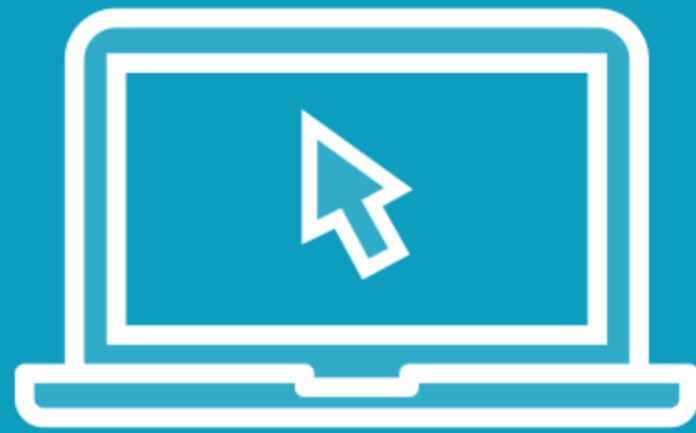
**Subject name is the device hostname**



**Enroll to TPM**



# Demo



## Device Certificate Template



# DC Certificate Template

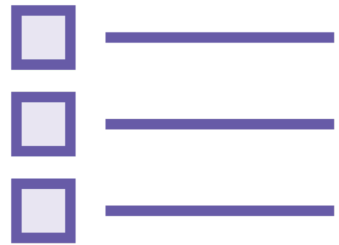
---



# Domain Controller Certificate Template



**Device certificate**



**Required EKUs: Client Authentication, Server Authentication, Smart Card Logon, KDC Authentication**



**Subject name is the server hostname**



**Deploy to all domain controllers**



**May already exist**





Demo



## Domain Controller Certificate Template



# Certificate Auto-enrollment

---



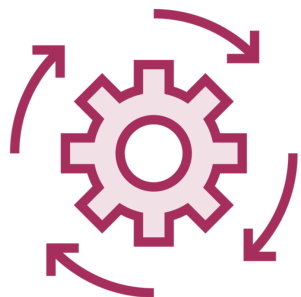
# Auto-enrollment GPO



**User and device certificates**



**Automatic provisioning**



**Automatic renewal!**



**Link at domain level**



# Demo



## Create certificate auto-enrollment GPO



# Summary



## Prepare the Infrastructure

### Summary

- Security groups
- Certificate templates
- Auto enrollment



Up Next:  
Configure VPN Infrastructure

---

