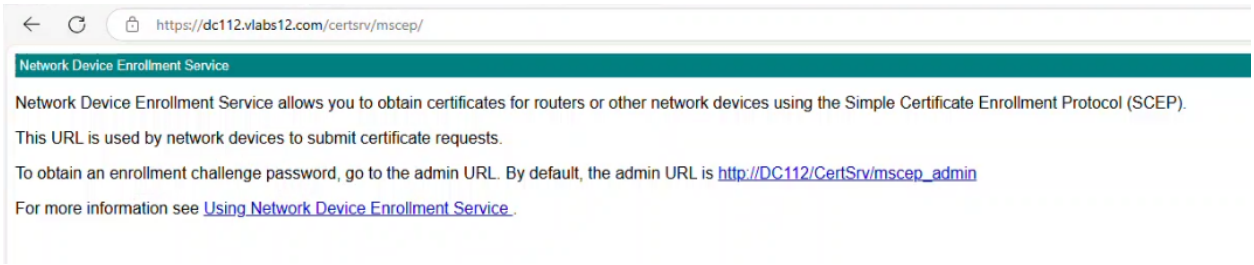

Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Cryptography\MSCEP"

```
PS C:\Users\Administrator.DC112> Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Cryptography\MSCEP"


SignatureTemplate      : IPSECIntermediateOffline
EncryptionTemplate     : IPSECIntermediateOffline
GeneralPurposeTemplate : IPSECIntermediateOffline
PSPath                 : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\MSCEP
PSParentPath           : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography
PSChildName            : MSCEP
PSDrive                : HKLM
PSProvider             : Microsoft.PowerShell.Core\Registry


PS C:\Users\Administrator.DC112>
```

Cisco Router config:

```
Enter configuration commands, one per line.  End with CNTL/Z.
Cisco-Router(config)#ip domain
Cisco-Router(config)#ip domain-name vlabs12.com
Cisco-Router(config)#service pas
Cisco-Router(config)#service password-encryption
Cisco-Router(config)#enable secret cisco
Cisco-Router(config)#crypto k
Cisco-Router(config)#crypto key g
Cisco-Router(config)#crypto key generate r
Cisco-Router(config)#crypto key generate rsa
The name for the keys will be: Cisco-Router.vlabs12.com
Choose the size of the key modulus in the range of 360 to 4096 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 0 seconds)

Cisco-Router(config)#username admin pri
Cisco-Router(config)#username admin privilege 15 secret cisco
Cisco-Router(config)#line vty 0 15
Cisco-Router(config-line)#transport
Cisco-Router(config-line)#transport input ssh
Cisco-Router(config-line)#
```

```
Cisco-Router(config-line)#login local
Cisco-Router(config-line)#exit
Cisco-Router(config)#ip ssh version 2
Cisco-Router(config)#_
```

SSH:

```
PS C:\Users\Administrator.DC112> ssh admin@192.168.12.50
The authenticity of host '192.168.12.50 (192.168.12.50)' can't be established.
RSA key fingerprint is SHA256:oIAmIOQEOEgIZTx8AtzLP5lrNoA/4Qgmae4JOK5JNLM.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.12.50' (RSA) to the list of known hosts.
Password:

Cisco-Router#
```

```
Cisco-Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Cisco-Router(config)#ip host dc112.vlabs12.com 192.168.12.1
Cisco-Router(config)#crypto key generate rsa label RouterKey modulus 2048
The name for the keys will be: RouterKey

% The key modulus size is 2048 bits
% Generating 2048 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 0 seconds)

Cisco-Router(config)#crypto pki trustpoint vlabs12-CA
Cisco-Router(ca-trustpoint)#enrollment url http://dc112.vlabs12.com/CertSrv/mscep/mscep.dll
Cisco-Router(ca-trustpoint)#enrollment mode ra
Cisco-Router(ca-trustpoint)#revocation-check crl
Cisco-Router(ca-trustpoint)#enrollment retry count 3
Cisco-Router(ca-trustpoint)#enrollment retry period 5
Cisco-Router(ca-trustpoint)#rsakeypair RouterKey 2048
Cisco-Router(ca-trustpoint)#usage ssl-client
Cisco-Router(ca-trustpoint)#fqdn Cisco-Router.vlabs12.com
Cisco-Router(ca-trustpoint)#exit
Cisco-Router(config)#crypto pki authenticate vlabs12-CA
Trustpoint 'vlabs12-CA' is a subordinate CA and holds a non self signed cert
Certificate has the following attributes:
       Fingerprint MD5: 441B240B BC2A488F B727910A A9DFC7CF
      Fingerprint SHA1: 53D8C88A 35D176F0 674617DB 811786D1 526B036A

% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
Cisco-Router(config)#
```

```
Cisco-Router(config)#crypto pki enroll vlabs12-CA
%
% Start certificate enrollment ..
% Create a challenge password. You will need to verbally provide this
   password to the CA Administrator in order to revoke your certificate.
   For security reasons your password will not be saved in the configuration.
   Please make a note of it.

Password:
Re-enter password:

% The subject name in the certificate will include: Cisco-Router.vlabs12.com
% Include the router serial number in the subject name? [yes/no]: yes
% The serial number in the certificate will be: 9MCUBS2SK9R
% Include an IP address in the subject name? [no]: no
Request certificate from CA? [yes/no]: yes
% Certificate request sent to Certificate Authority
% The 'show crypto pki certificate verbose vlabs12-CA' commandwill show the fingerprint.

Cisco-Router(config)#end
Cisco-Router#wr
Building configuration...
[OK]
Cisco-Router#
```

```
CA Certificate
  Status: Available
  Version: 3
  Certificate Serial Number (hex): 7B000000003442ED6A8223ED505000000000003
  Certificate Usage: Signature
  Issuer:
    cn=Root12CA
  Subject:
    cn=vlabs12-CA
    dc=vlabs12
    dc=com
  CRL Distribution Points:
    http://dc112.vlabs12.com/CertEnroll/Root12CA.crl
  Validity Date:
    start date: 12:58:56 UTC May 28 2025
    end   date: 23:30:29 UTC May 27 2030
  Subject Key Info:
    Public Key Algorithm: rsaEncryption
    RSA Public Key: (4096 bit)
  Signature Algorithm: SHA256 with RSA Encryption
  Fingerprint MD5: 441B240B BC2A488F B727910A A9DFC7CF
  Fingerprint SHA1: 53D8C88A 35D176F0 674617DB 811786D1 526B036A
  X509v3 extensions:
    X509v3 Key Usage: 86000000
      Digital Signature
      Key Cert Sign
      CRL Signature
    X509v3 Subject Key ID: 888DA2B9 38BC98FB BD7FC278 CB0C3100 701DDBEF
    X509v3 Basic Constraints:
        CA: TRUE
    X509v3 Authority Key ID: BD526E47 458BA40A 7684E69B 1057430E 3A9BC41F
    Authority Info Access:
```

```
Associated Trustpoints: vlabs12-CA
Storage: nvram:Root12CA#3CA.cer
```

```
PS C:\Users\Administrator.DC112> certutil -view -restrict "CommonName=Cisco-Router.vlabs12.com"
Schema:
  Column Name                     Localized Name                  Type    MaxLength
  ------------------------------  ------------------------------  ------  ---------
  Request.RequestID               Request ID                      Long    4 -- Indexed
  Request.RawRequest              Binary Request                  Binary  65536
  Request.RawArchivedKey          Archived Key                    Binary  65536
  Request.KeyRecoveryHashes       Key Recovery Agent Hashes       String  8192
  Request.RawOldCertificate       Old Certificate                 Binary  16384
  Request.RequestAttributes       Request Attributes              String  32768
  Request.RequestType             Request Type                    Long    4
  Request.RequestFlags            Request Flags                   Long    4
  Request.StatusCode              Request Status Code             Long    4
  Request.Disposition             Request Disposition             Long    4 -- Indexed
  Request.DispositionMessage      Request Disposition Message     String  8192
  Request.SubmittedWhen           Request Submission Date         Date    8 -- Indexed
  Request.ResolvedWhen            Request Resolution Date         Date    8 -- Indexed
  Request.RevokedWhen             Revocation Date                 Date    8
  Request.RevokedEffectiveWhen    Effective Revocation Date       Date    8 -- Indexed
  Request.RevokedReason           Revocation Reason               Long    4
  Request.RequesterName           Requester Name                  String  2048 -- Indexed
  Request.CallerName              Caller Name                     String  2048 -- Indexed
  Request.SignerPolicies          Signer Policies                 String  8192
  Request.SignerApplicationPolicies  Signer Application Policies   String  8192
  Request.Officer                 Officer                         Long    4
  Request.DistinguishedName       Request Distinguished Name      String  8192
  Request.RawName                 Request Binary Name             Binary  4096
  Request.Country                 Request Country/Region          String  8192
  Request.Organization            Request Organization            String  8192
  Request.OrgUnit                 Request Organization Unit       String  8192
  Request.CommonName              Request Common Name             String  8192
  Request.Locality                Request City                    String  8192
  Request.State                   Request State                   String  8192
  Request.Title                   Request Title                   String  8192
  Request.GivenName               Request First Name              String  8192
```