3 Setting Up VPN Login

This section describes what you need to prepare before you can use the VPN Login action.

3.1 Supported VPN Clients

Intel Authenticate supports VPN clients that use the standard Microsoft Cryptographic Application Programming Interface (CAPI) to the Credential Service Provider (CSP). These specific VPN clients were tested and validated to work with Intel Authenticate:

- Cisco*
- Microsoft*
- Juniper*

3.2 Intel IPT with PKI

The VPN Login action uses certificates generated and protected in the hardware of the Intel platform using Intel IPT with PKI. Components of Intel IPT with PKI are required:

- **On the client platform** – The Intel Authenticate installer automatically installs this component on the client platforms. (If a platform supports Intel Authenticate, then it supports Intel IPT with PKI.) No further action is required.
- **On the Microsoft CA** – See Preparing the Certification Authority below.

> **Note:**
>
> Intel Authenticate requires version 4.1 or higher of Intel IPT with PKI. Earlier versions of Intel IPT with PKI are not supported.

3.3 Preparing the Certification Authority

A Microsoft Certification Authority (CA) is necessary if you want to use Enterprise CA templates when generating certificates for the VPN Login action. Before you can define the template, you need to install a set of "CA Components" for Intel IPT with PKI on the server where your organization's CA is located. This section describes the prerequisites for the CA and how to install the CA Components.

3.3.1 Supported Server Operating Systems

The CA Components of Intel IPT with PKI are supported on these server operating systems:

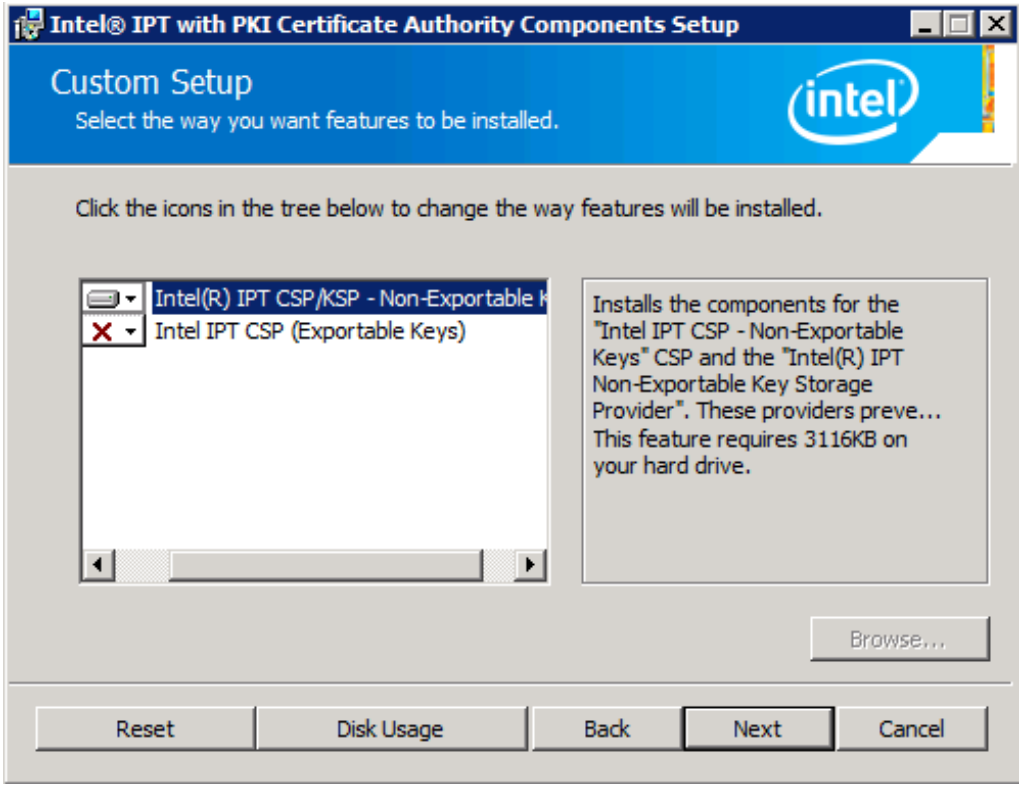
- Windows Server 2012 R2
- Windows Server 2012
- Windows Server 2008 R2

3.3.2 Installing the CA Components

The installer for the CA Components of Intel IPT with PKI is located in the `MS_CA_Installer` folder in the root of this package. You can install Intel IPT with PKI using the installer wizard or a CLI command.

To install the CA Components of Intel IPT with PKI (using the wizard):

1. On your Certificate Authority server, double-click **Intel_IPT_PKI_CA_Components_x64**. The Welcome window opens.
2. Click **Next**. The End User License Agreement window opens.
3. Select **I accept the terms in the License Agreement** and click **Next**. The Custom Setup window opens.



4. By default, the "Intel IPT CSP/KSP Non-Exportable Keys" option is selected. This is the only option that you need to install to enable the VPN Login action. Click **Next** and then click **Install** to start the installation.

To silently install the CA Components of Intel IPT with PKI:

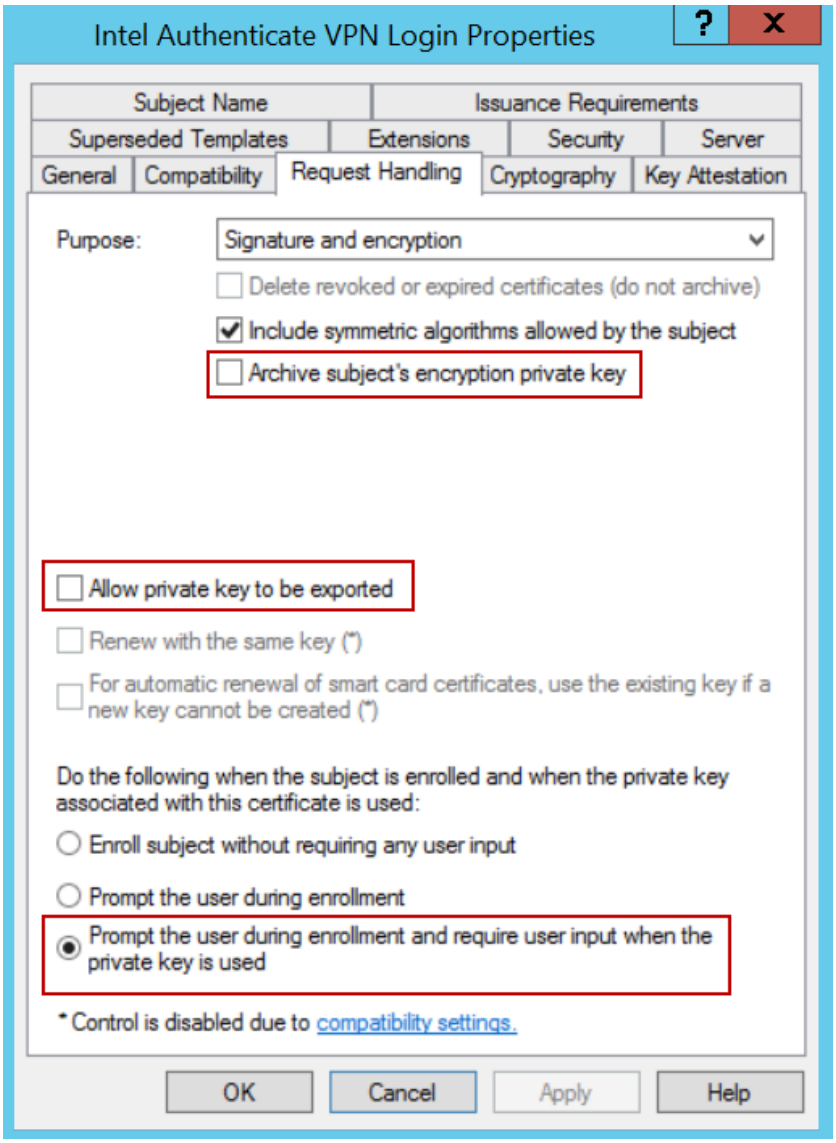
1. On the server where the CA is located, open an administrative command prompt.
2. Enter this command:

```
msiexec /i [installer_filename].msi /qn ADDLOCAL=NonExportable
```

3.4 Defining the CA Template for VPN Login

The steps to create a certificate template vary between different versions of the Windows Server operating system. In addition, the value of many settings depend on the specific requirements of your organization. This section describes the template settings that have specific requirements for the VPN Login action.

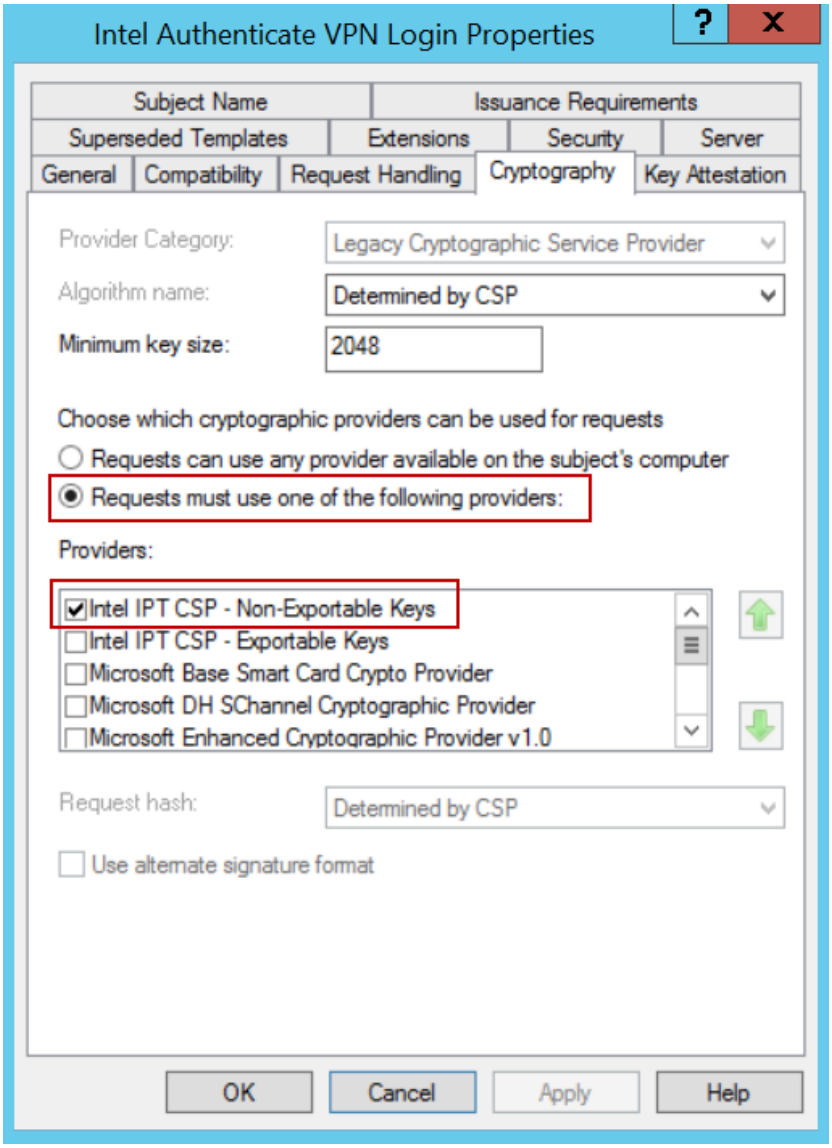
Request Handling



In the Request Handling tab:

- Make sure that the **Archive subject's encryption private key** check box is NOT selected. Selecting this option will cause the enrollment to fail with an "invalid parameter" error message.
- Make sure that the **Allow private key to be exported** check box is NOT selected.
- Select the option: **Prompt the user during enrollment and require user input when the private key is used**.

CSP Selection / Cryptography



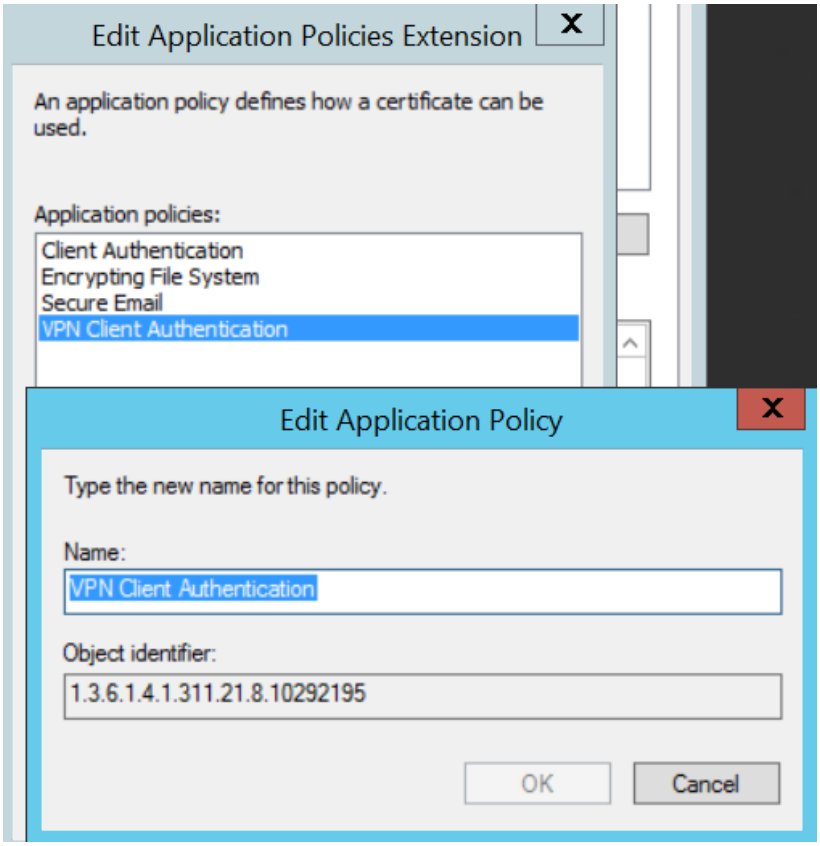
When selecting the CSP, you must make sure that only the check box of this CSP is selected:

- Intel IPT CSP - Non-Exportable Keys

Note:

Intel IPT with PKI includes additional CSPs and KSPs. These additional CSPs and KSPs are not supported when using the VPN Login action. This also means that version 3 templates are not supported (because they do not support CSPs.)

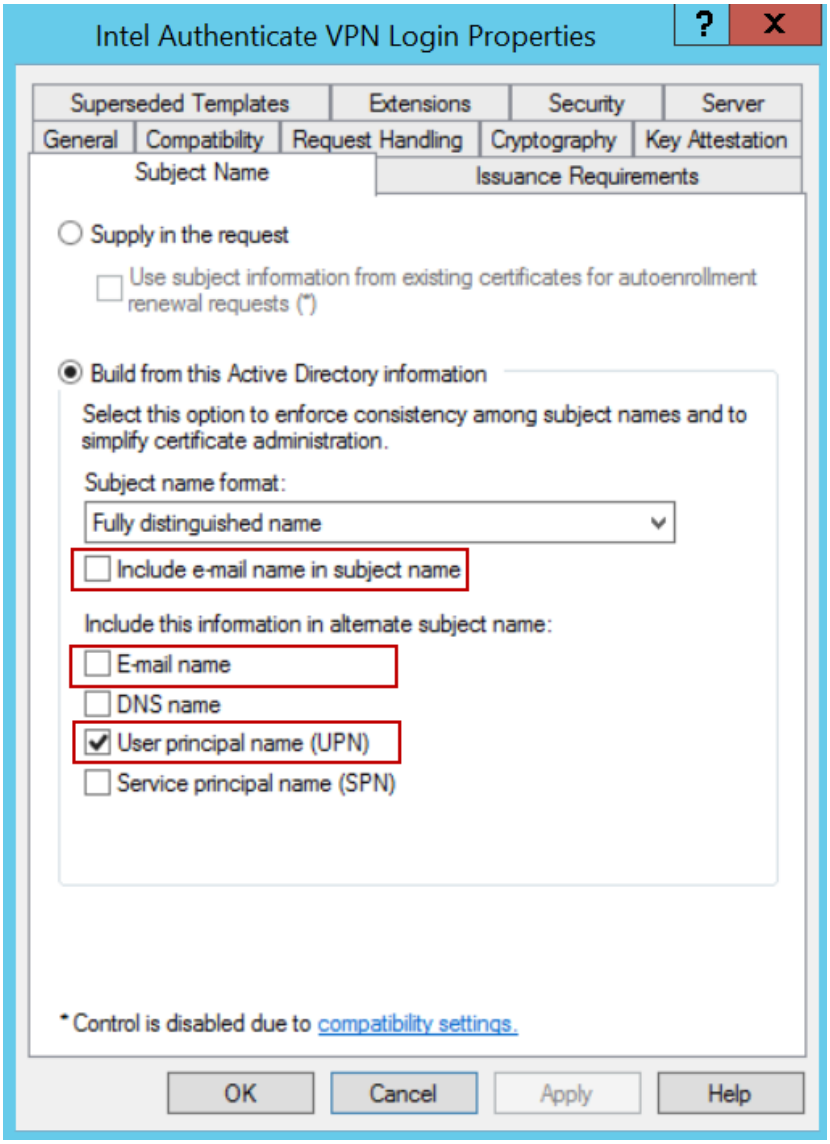
Application Policy Extension



In the Extensions tab:

- Add an application policy extension specifically for the VPN Login action.
- Define a unique Object Identifier (OID) that will be used to identify this policy. This is the OID that you will need to configure in your organization's VPN appliance. Check the maximum number of characters supported by your VPN appliance. (Many VPN appliances limit the size of the OID to less than 30 characters.)

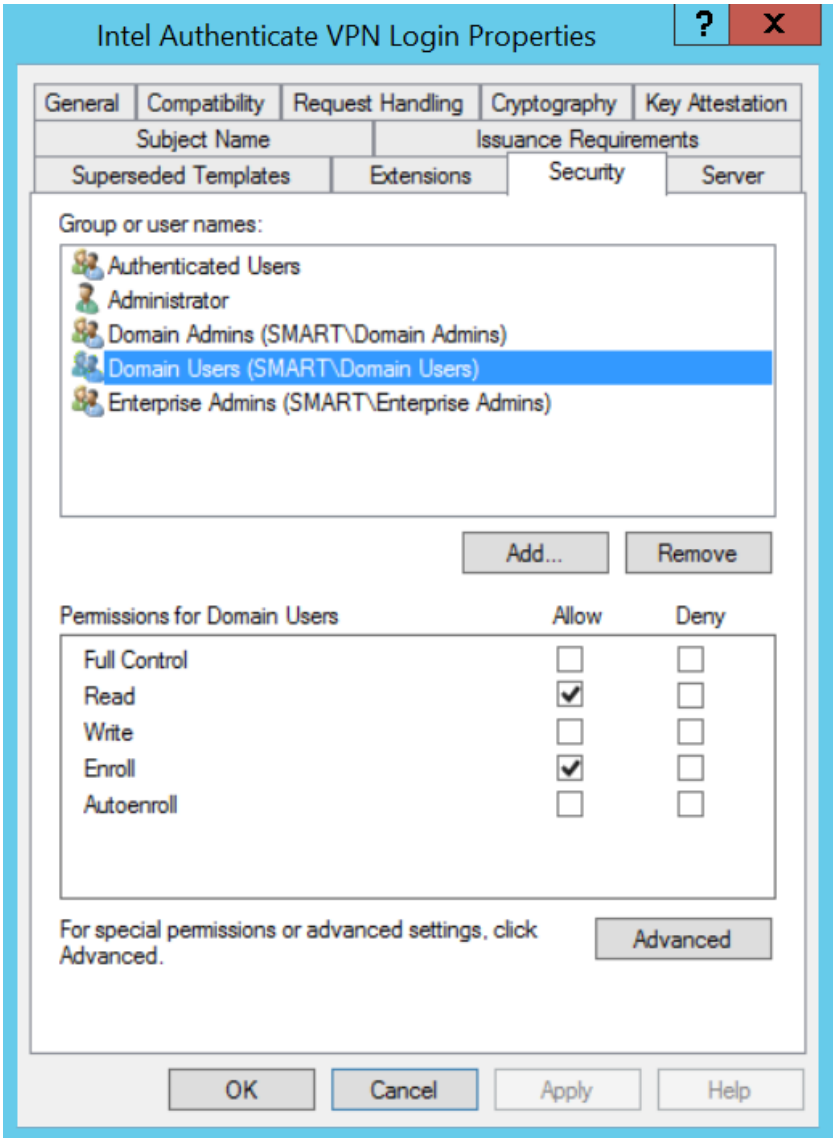
Subject Name



In the Subject Name tab,

- Make sure that the **User principal name (UPN)** check box is selected
- If your user accounts are defined in Active Directory without email accounts, make sure that both these check boxes are NOT selected:
  - **Include e-mail name in alternate subject name**
  - **E-mail name**

Security Tab



In the Security tab, make sure that all the user groups that you want to have access to the VPN certificate are defined with these permissions:

- **Read**
- **Enroll**

3.5 Configuring the VPN Appliance

To use the VPN Login action, you must configure your VPN appliance to require certificates instead of passwords. When you define the certificate details in the VPN appliance, make sure that you use the OID that you created specifically for the VPN Login action. For instructions how to define your VPN appliance to use certificates, refer to the documentation supplied with your VPN appliance.

3.6 Generating a Certificate on the Client

Each user account that will use the VPN Login action requires a certificate, based on the VPN Login template, to be installed in the certificate store of the user. During installation of Intel Authenticate, a utility named `CertificateUtility.exe` is installed on each platform. The utility is installed in this folder: `C:\Program Files\Intel\Intel(R) Identity Protection Technology with PKI`. You can use this utility to generate the certificate on the client platforms.

This is the syntax to create a certificate for VPN Login:

```
CertificateUtility.exe -c create_cert [-a <action name>] [-u <ca_url>]
[-t <template name>] [-i <yes|no>]
```

Flag	Details
`-a <action_name>`	Valid values when generating a certificate for VPN Login: • **Unattended_VPNLogin** – The user is not required to provide any input when the certificate is installed. This option also enables you to install the certificate on the platform before the user has enrolled their factors. • **VPNLogin** – During installation of the certificate, the user must authenticate using the factors defined for the VPN Login action. If authentication fails, the certificate will not be installed. Using this option means that you cannot install the certificate until after the user has enrolled their VPN Login factors. **Note:** The value you define in this flag depends on what you defined in the VPN Login action in the Intel Authenticate policy. To use the `Unattended_VPNLogin` option, you must first enable this option in the policy.
`-u <ca_url>`	The certificate authority URL. If not supplied, the tool will loop over all CAs found on the domain and try to send the request to each one.
`-t <template_name>`	The name of the VPN certificate template. Make sure that you spell the name exactly as you defined it in the certificate template. If you do not supply a name, the default for VPN Login is: `IntelAuthenticateVPNLogin`.
`-i <yes|no>`	Defines if the user must be authenticated when the certificate is used. The default setting is `no`. **Note:** For VPN Login you must always set this parameter to `yes`.

Example #1: Generating a certificate that does not require user input during installation:

```
CertificateUtility.exe -c create_cert -a Unattended_VPNLogin -t <My_VPN_Template>
-i yes
```

Example #2: Generate a certificate that requires the user to authenticate during installation:

```
CertificateUtility.exe -c create_cert -a VPNLogin -t <My_VPN_Template> -i yes
```