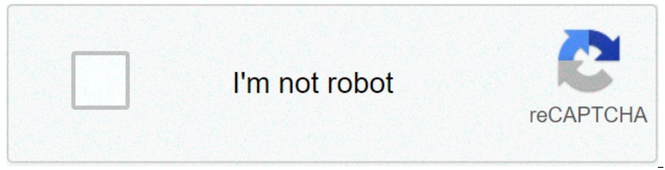

Continue

Domain controller certificate template

Sep 06, 2010 When you install the Windows 2008 Certification Authority certificate template a new domain controller named Kerberos Authentication is available. This replaces the Domain Controller Authentication template. If you need more information about a new certificate template that was sent with a Windows 2008 CA, you can read this article. Here is a tab that describes the specific attributes of Domain Controller Authentication and the Kerberos Authentication template: Kerberos Domain Controller Authentication Key Authentication Server Authentication Smart Card Logon Client Authentication Smart Card Logon KDC Authentication Server Authentication. Subject Alternate Name DNS Name : Domain Controller FQDN. DNS Name : Domain FQDN. DNS Name : NetBios Domain Name. For more information about using the KDC Authentication key that helps ensure that smart card users authenticate against valid Kerberos domain controllers, you can read this document: Enable Strict KDC Validation in Windows Kerberos. Having a domain name rather than a domain controller name in the Alternate Name Subject certificate proves that the computer that presents the certificate is the domain controller for the domain that is contained in the Subject Alternative Name. The domain name must also be included in the certificate to enable Strict KDC Validation. We'll explain how to use the Kerberos Authentication template certificate on your domain controller and how to revoke an old certificate issued with the Domain Controller Authentication template after it's useless. We distribute certificates to domain controllers using autoenrollment, to achieve this you need to configure your templates (permissions, settings...) and set up GPOs. If you want a new Kerberos Authentication template to replace the Domain Controller Authentication template, you need to configure it using certtmpl.msc by setting up the Superseded Templates tab. For more information, you can see the Replace Certificate Template chapter of this article. Once the template is configured properly and ready for autoenrollment, the new certificate will be used automatically, you can run the certutil -pulse command on the domain controller, to speed up the autoenrollment process. The new domain controller certificate is replaced in the local computer store, a message with the Source AutoEnrollment is displayed in the eventlog that tells us that the Kerberos Authentication certificate is installed. With Quest ActiveRoles Management Shell for Active Directory v1.4, you can manage certificates using PowerShell thanks to Certificate Management CmdLet and PKI. First we will check that the Kerberos Authentication certificate is installed on each Domain Controller: Get-QADComputer -computerRole 'DomainController' | Get-QADCertificate -Revoked:$false -template:'*kerberos authentication*' | table-format template,IssuedTo -autosizeGet-QADComputer | Get-QADCertificate -Revoked:$false -template:'*kerberos authentication*' | Template format-table,IssuedTo -autosize After all your domain controllers have registered a new Kerberos Authentication certificate and you have checked everything is running correctly, you can disable the old Domain Controller Authentication template with certsrv.msc to avoid installing this kind of certificate on domain controllers. Then you can revoke the old Domain Controller Authentication certificate that replaces the Kerberos Authentication certificate. To achieve that, we'll combine the Quest CmdLets and certutil -revoke commands. You just need to retrieve the serial number of the Domain Controller Authentication certificate and specify the reason code for the revocation of this certificate: In our case 4 to Superseded: Get-QADComputer -computerRole 'DomainController' | Get-QADCertificate -Revoked:$false -template:*domain controller authentication* | foreach {certutil -config %SRV_CA_FQDN%\%CA_Common_Name% -revoke $_. SerialNumber 4}Get-QADComputer -computerRole 'DomainController' | Get-QADCertificate -Revoked:$false -template:*domain controller authentication* | foreach {certutil -config %SRV_CA_FQDN%\%CA_Common_Name% -revoke $_. SerialNumber 4} You just need to adapt: %SRV_CA_FQDN%: Publish server CA FQDN. %CA_Common_Name%: Certification Authority General Name. By combining certutil command line tools and Quest AD CmdLets v1.4, you can create some of your PKI management tasks automatically. This post is also available in: France There may be two inputs to this issue: Part 1: Template supercedence In the certificate template settings (certtmpl.msc), there is a Superseded Templates tab, where you can specify a list of templates that replace the current template. This setting is only used by the certificate autoenrollment feature. During autoenrollment, the client checks each template and checks whether the current template is listed as *superseded* in another template. If listed, the template is currently skipped. This behavior is defined in the protocol specification [MS-CAESO], •4.4.5.6.1: 4.4.5.6.1 Specifies whether the CertificateTemplate Instance is Valid for Autoenrollment If any of the conditions in the following list are true, autoenrollment SHOULD NOT process new registrations for certain CertificateTemplate instances <... > skipped for brevity There is an instance of CertificateTemplate in the CertificateEnrollmentPolicy.Templates list whose certificateTemplate.SupersededTemplates list contains the same value as the current CertificateTemplate.CommonName Note: In 2014, the Document [MS-CAESO] was terminated and its content was moved to a number of other protocol specifications and I have not tried to track this step. Given that nothing has been changed since then, you can use an archived PDF copy of the document: An archived pdf copy of [MS-CAESO]. This answers the first half of the question: why is it allowed for templates not automated. Thus, check if there is no configured to replace the Domain Controller Authentication template. If anything like it, remove it from the superseded list. And check whether Domain Controller Authentication is added for publishing to a CA that is enabled for web registration. Part 2: Ms-XCEP Cache When clients use the Certificate Enrollment Web Service (Microsoft CEP/CES), they do the following: Connect to service registration policy (CEP) and request policy. CEP authenticates clients and reads all certificate templates from Active Directory where authenticated entities have at least Read permissions. CEP contacts the CA to obtain a list of templates allowed by each CA and builds a response as specified in [MS-XCEP] •3.1.4.1.3.23 The response message has NextUpdateHours that is: An integer that represents the number of hours that the server recommends the client wait before sending another GetPolicies message. The default value is 8 hours. The client caches this response and may not try to request a new policy with the list of templates updated for this time period. Although, there is a booleanNotChanged field policy that can be used by the client to poll for changes, but from practice I can tell that the client is not doing the polling. Instead, they use these bits to determine whether the cache policy should be replaced or not. This is just my opinion, because every policy change has great latency on the client. Either, wait at least 8 hours and see if the problem is resolved automatically when the client retrieves a new policy from the CEP server or tries to force policy retrieval: Remove all content from %systemdrive%\ProgramData\Microsoft\Windows\X509Enrollment on the target computer (DC) and then run certutil -pulse to trigger autoenrollment. During this call, the new policy will be downloaded and autoenrollment should retrieve the correct template. In fact, you have three possibilities: Domain Controllers (Windows Server 2000) Domain Controller Authentication (Windows Server 2003) Kerberos Authentication (Windows Server 2008 and above) This explanation comes from Russell Tomkins Field of Microsoft Premier Engineers in an excellent post that you can find here: Create a Custom Secure LDAP Certificate for Domain Controllers with Auto Renewal Watch 138 Star 984 Fork 1.4k You cannot perform that action at this time. You sign in with another tab or window. Reload to refresh your session. You exit in another tab or window. Reload to refresh your session. We use optional third-party analytics cookies to understand how you use GitHub.com that can build better products. Learn more. We use optional third-party analytics cookies to understand how you use GitHub.com that can build better products. You can always update your options by clicking Preferences at the bottom of the page. For more information, see our Privacy Statement. We use important cookies to perform important website functions, for example they are used to log in. Learn more Always on We use analytics cookies to understand how you use our website so we can make it better, better, they are used to collect information about the pages you visit and how many clicks you need to complete the task. Learn more