PKI Certificate Settings

https://campus.barracuda.com/doc/73719508/

For each PKI certificate, you can view and edit the settings in the following sections:

General Settings

Setting	Setting Description	Options
Keysize in Bits	Specifies the key size in bits. Normally the value ranges from 512 to 4096 bits (default: **1024**). The key size must be at least 1024 bits for end-user certificates. When the lifetime of the CA is 10 years or longer, the key size must be at least 2048 bits (Recommended: **4096**).	• 512 • 1024 (Default) • 2048 • 4096
Duration of Validity	In days, specifies how long the certificate remains valid (default*: 5000*). For example, enter *5475* days for a root certificate that will remain valid for 15 years (365 * 15).	
Key Algorithm	Specifies the algorithm used for key creation	• rsa (Default) • dsa
Key Encryption	Specifies the algorithm used for key encryption	• TripleDES (Default) • IDEA • DES
Message Digest Algorithm	Specifies the hash algorithm	• md2 • md5 • mdc2 • sha1 (Default)
Password	Defines the certificate password.	
Validate Password	Validates the certificate password.	

Subject

Setting	Setting Description
Common Name	Specifies the name of the certificate. (Do not use special characters and underscores in the common name!)
Email Address	Specifies the email address of the certificate owner
Country State or Province / Locality / Organisation / Organisation Unit	Specifies the address of the organization.

V3 Extensions

For more information on V3 extensions, see RFC 3280 at http://www.ietf.org/rfc/rfc3280.txt.

If you select the **Critical** check box for an application, the application must use V3 extensions. The certificate may then only be used as specified in the **keyUsage** and **extendedKeyUsage** settings.

Setting	Setting Description	OID/CANBECRIT	Values
basicConstraints	Defines whether the certificate is a CA (*CA:true*) or not (*CA:false - default*). The CA boolean indicates whether the certified public key belongs to a CA. If the CA boolean is not asserted, then the keyCertSign bit in the key usage extension MUST NOT be asserted.	`OID = 2.5.29.19` `CANBECRIT=true`	• true • false
keyUsage	Specifies the purpose of the key contained in the certificate. This extension is useful when the key can be used for more than one operation.	`OID = 2.5.29.15`	**BIT STRING** • digitalSignature - (0) • nonRepudiation - (1) • keyEncipherment - (2) • dataEncipherment - (3) • keyAgreement - (4) • keyCertSign - (5) • cRLSign - (6) • encipherOnly - (7) • decipherOnly - (8) • 0) sign for entity authentication and data origin authentication with integrity 1) sign with anon-repudiation service. • 2) encrypt keys for transport using RSA like algorithms. • 3) encrypt data. • 4) exchange keys using D-H like algorithms. • 5) sign certificates. • 6) sign CRLs. • 7) encrypt data using D-H like algorithms. • 8) decrypt data using D-H like algorithms.

extendedKeyUsage	Indicates one or more purposes for which the certified public key may be used, in addition to purpose specifies by the keyUsage extension. In general, this extension is only used in end entity certificates.	`OID = 2.5.29.37` `CANBECRIT=true`	• serverAuth • clientAuth • emailProtection • codeSigning • timeStamping • OCSPSigning • smarCardLogon • secureMail • msCodInd (MS Individual Code Signing) • msCodeCom (MS Commercial Code Signing) • msCTLSign (MS Trust List Signing) • msSGC (MS Server Gated Cryptography) • msEFS (MS Encrypted File System)
subjectKeyIdentifier	Hash of the subject. This extension provides a means of identifying certificates that contain a particular public key.	`OID = 2.5.29.14` `CANBECRIT=false`	hash
authorityKeyIdentifier	Specifies the public key that is used to verify the signature on this certificate or CRL.	`OID = 2.5.29.35` `CANBECRIT=false`	• keyid:always • keyid:copy • issuer:always • issuer:copy
authorityInfoAccess	Indicates how to access CA information and services for the issuer of the certificate in which the extension appears. Information and services may include online validation services and CA policy data. (The location of CRLs is not specified in this extension; that information is provided by the cRLDistributionPoints extension.) This extension may be included in end entity or CA certificates, and it MUST be non-critical.	`OID = 1.3.6.1.5.5.5.7.1.1`	A string. For example: OCSP;URI: `ocsp.my.host/` or calssuers;URI: `my.ca/ca.html`

subjectAltName	Specifies additional identities that are bound to the subject of the certificate. You can specify an email address, a DNS name, an IP address, a uniform resource identifier (URI), MS Domain GUID, or MS Domain User.	`OID = 2.5.29.17` `CANBECRIT=true`	• Email - enter an email address or "copy" for copying from subject • DNS • URI • IP • MS Domain GUID - for Smartcard Server • MS Domain User - for Smartcard User
issuerAltName	Associates Internet-style identities with the certificate issuer.	`OID = 2.5.29.18` `CANBECRIT=true`	issuer:copy

crlDistributionPoints	Specifies the distribution points for the Certificate Revocation List (CRL).	`OID = 2.5.29.31`
		This lists the distribution points for CRLs.
			Example:
			`ldap://some.ldap-test.eu/cn=rootcert,dc=ldap-test,dc=eu`
			`some.ldap-test.eu/crl/rootcert.crl`

DomainController	Specifies a Microsoft-specific extension for entering DomainControllers.	`OID = 1.3.6.1.4.1.311.20.2` This is a Microsoft specific extension needed for smartcard login.	• Machine- For a machine • SmartCardLogon - For a user (logon) • SmartCardUser - For a user (logon and email)
nsCert Type	Specifies a Netscape certificate type.		• client • server • email • objsign • sslCA • emailCA • objCA
nsComment	Enables you to enter comments.	`OID = 2.16.840.1.113730.1.13`	Just an extension to provide a possibility for a comment. This is an old Netscape extension.