

## PKI Certificate Settings

<https://campus.barracuda.com/doc/79463198/>

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

### General Settings

Setting	Setting Description	Options
<b>Keysize in Bits</b>	Specifies the key size in bits. Normally the value ranges from 512 to 4096 bits (default: <b>1024</b> ). 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: <b>4096</b> ).	<ul style="list-style-type: none"> <li>• 512</li> <li>• 1024 (Default)</li> <li>• 2048</li> <li>• 4096</li> </ul>
<b>Duration of Validity</b>	In days, specifies how long the certificate remains valid (default: <i>5000</i> ). For example, enter <i>5475</i> days for a root certificate that will remain valid for 15 years (365 * 15).	
<b>Key Algorithm</b>	Specifies the algorithm used for key creation	<ul style="list-style-type: none"> <li>• rsa (Default)</li> <li>• dsa</li> </ul>
<b>Key Encryption</b>	Specifies the algorithm used for key encryption	<ul style="list-style-type: none"> <li>• TripleDES (Default)</li> <li>• IDEA</li> <li>• DES</li> </ul>
<b>Message Digest Algorithm</b>	Specifies the hash algorithm	<ul style="list-style-type: none"> <li>• md2</li> <li>• md5</li> <li>• mdc2</li> <li>• sha1 (Default)</li> </ul>
<b>Password</b>	Defines the certificate password.	
<b>Validate Password</b>	Validates the certificate password.	

### Subject

Setting	Setting Description
<b>Common Name</b>	Specifies the name of the certificate. (Do not use special characters and underscores in the common name!)
<b>Email Address</b>	Specifies the email address of the certificate owner
<b>Country State or Province / Locality / Organisation / Organisation Unit</b>	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
<b>basicConstraints</b>	Defines whether the certificate is a CA ( <i>CA:true</i> ) or not ( <i>CA:false - default</i> ). 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	<ul style="list-style-type: none"> <li>• true</li> <li>• false</li> </ul>
<b>keyUsage</b>	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	<b>BIT STRING</b> <ul style="list-style-type: none"> <li>• digitalSignature - (0)</li> <li>• nonRepudiation - (1)</li> <li>• keyEncipherment - (2)</li> <li>• dataEncipherment - (3)</li> <li>• keyAgreement - (4)</li> <li>• keyCertSign - (5)</li> <li>• cRLSign - (6)</li> <li>• encipherOnly - (7)</li> <li>• decipherOnly - (8)</li> <li>• 0) sign for entity authentication and data origin authentication with integrity 1) sign with anon-repudiation service.</li> <li>• 2) encrypt keys for transport using RSA like algorithms.</li> <li>• 3) encrypt data.</li> <li>• 4) exchange keys using D-H like algorithms.</li> <li>• 5) sign certificates.</li> <li>• 6) sign CRLs.</li> <li>• 7) encrypt data using D-H like algorithms.</li> <li>• 8) decrypt data using D-H like algorithms.</li> </ul>

<b>extendedKeyUsage</b>	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	<ul style="list-style-type: none"> <li>• serverAuth</li> <li>• clientAuth</li> <li>• emailProtection</li> <li>• codeSigning</li> <li>• timeStamping</li> <li>• OCSPSigning</li> <li>• smarCardLogon</li> <li>• secureMail</li> <li>• msCodInd (MS Individual Code Signing)</li> <li>• msCodeCom (MS Commercial Code Signing)</li> <li>• msCTLSign (MS Trust List Signing)</li> <li>• msSGC (MS Server Gated Cryptography)</li> <li>• msEFS (MS Encrypted File System)</li> </ul>
<b>subjectKeyIdentifier</b>	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
<b>authorityKeyIdentifier</b>	Specifies the public key that is used to verify the signature on this certificate or CRL.	OID = 2.5.29.35 CANBECRIT=false	<ul style="list-style-type: none"> <li>• keyid:always</li> <li>• keyid:copy</li> <li>• issuer:always</li> <li>• issuer:copy</li> </ul>
<b>authorityInfoAccess</b>	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: ojsp.my.host/ or calssuers;URI: my.ca/ca.html

<b>subjectAltName</b>	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	<ul style="list-style-type: none"> <li>• Email - enter an email address or "copy" for copying from subject</li> <li>• DNS</li> <li>• URI</li> <li>• IP</li> <li>• MS Domain GUID - for Smartcard Server</li> <li>• MS Domain User - for Smartcard User</li> </ul>
<b>issuerAltName</b>	Associates Internet-style identities with the certificate issuer.	OID = 2.5.29.18 CANBECRIT=true	issuer:copy
<b>crlDistributionPoints</b>	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
<b>DomainController</b>	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.	<ul style="list-style-type: none"> <li>• Machine- For a machine</li> <li>• SmartCardLogon - For a user (logon)</li> <li>• SmartCardUser - For a user (logon and email)</li> </ul>
<b>nsCert Type</b>	Specifies a Netscape certificate type.		<ul style="list-style-type: none"> <li>• client</li> <li>• server</li> <li>• email</li> <li>• objsign</li> <li>• sslCA</li> <li>• emailCA</li> <li>• objCA</li> </ul>
<b>nsComment</b>	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.

© Barracuda Networks Inc., 2019 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.