ORDER No.11ee
IO

Service Manual

AUTOMOTIVE ELECTRONICS

MAZDA
CA-DM4491K

Main Display Unit [Center Panel Module System]

PART No. :
VEHICLE : Mazda 6
DESTINATION : USA
PRODUCED AFTER : June, 2004

Specifications*

Clock Display	12H/24H display
Outside Air Temperature Display	
<North America>	Fahrenheit display
<Except for North America>	Centigrade display
DIS Display Unit	
<Instantaneous Mileage>	L/100km (Mile zone : L/100mile)
<Average Mileage>	L/100km (Mile zone : L/100mile)
<The Balance of Mileage>	km (Mile zone : mile)
<Average Car Speed>	km/h (Mile zone : mile/h)
Dimensions** (W×H×D)	270.3 × 41.6 × 57.4 (mm)
Weight**	270g

* Specifications and the design are subject to possible modification without notice due to improvements.
** Dimensions and Weight shown are approximate.

CONTENTS

Manufactured for MAZDA
by Matsushita Electric Industrial Co., LTD.

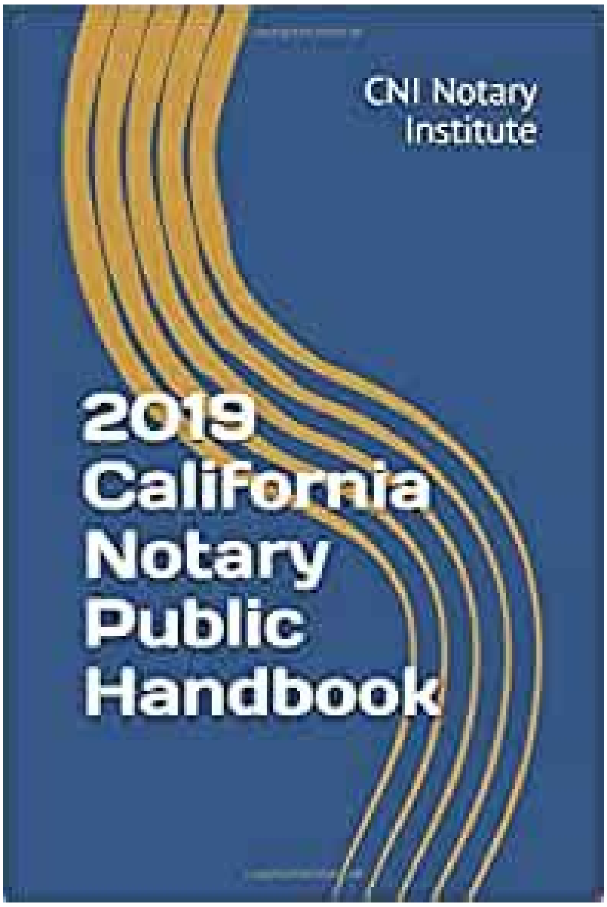
File Name: ca view manual.pdf
Size: 1698 KB
Type: PDF, ePub, eBook
Category: Book
Uploaded: 14 May 2019, 12:25 PM
Rating: 4.6/5 from 600 votes.

Book Descriptions:

We have made it easy for you to find a PDF Ebooks without any digging. And by having access to our ebooks online or by storing it on your computer, you have convenient answers with ca view manual . To get started finding ca view manual , you are right to find our website which has a comprehensive collection of manuals listed.
Our library is the biggest of these that have literally hundreds of thousands of different products represented.

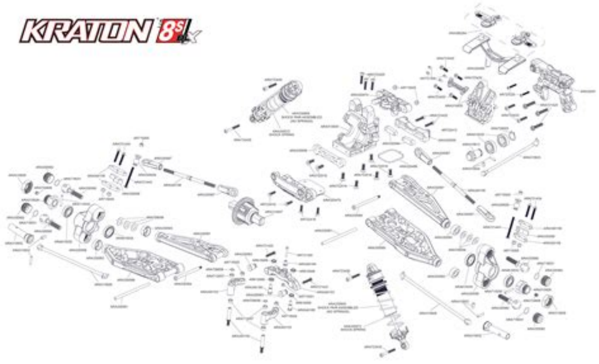
Book Descriptions:

ca view manual

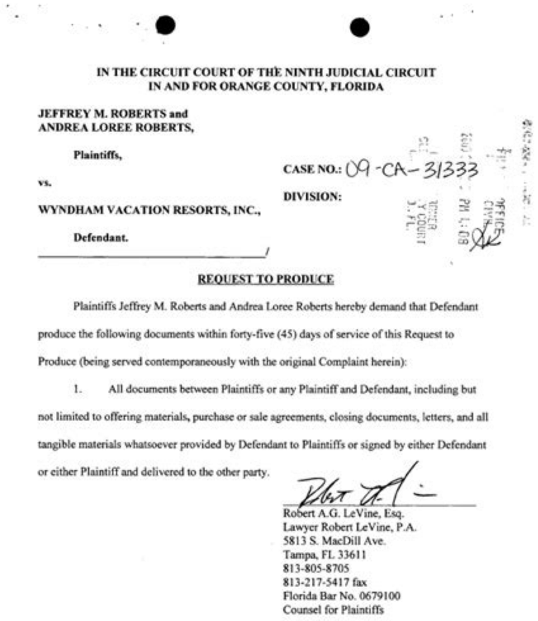


Clients should consider CAView as an alternative to storing listings for their retention needs. Since any computer output can be specified for archival, CAView is especially wellsuited to the management of production JCL listings and production reports. CAView is available on the Gold Camp and Vacaville z Systems through specific individualized CAView database repositories based on client departments. Although the main purpose is to provide an alternative method of storing and retaining computer output, CAView may also be used for AFP to PDF transformation and PDF collection for output that will also be stored in the CAView database. The storage and retention specifications of output is dependent upon the needs of the client CAView database repositories. Typically, each day is considered a generation. The clients can access their outputs via TSO CLISTS, CICS Crossmemory services, ISPF menu selections, or WebViewer URL. The first field on the selection menu is SYSOUT ID, which by default is the same as the jobname.For GENERATION, you can enter a generation number or range of generation numbers e.g. 640643. CAView assigns a sequential generation number for each day. You can alternatively enter a relative generation number or range of numbers e.g., a range of 30 would cover all jobs archived during the period beginning 3 generations ago through the current generation. A relative date or range of dates can also be specified. If nothing is entered in either the GENERATION or the DATE fields, only the current generation is searched for eligible archived output. Depending on the CAView database repository, there are different security mechanisms that are deployed. These will determine whether the user can do within a given CAView database repository. Possible exception codes may include SB37, U0024, 0016 condition code and JCLERR. This command is used to copy output that has already been archived to tape into a temporary disk file so the output can be browsed.https://etudemichel.fr/upload/deus-lo-vult-6_2-manual.xml

- **ca view manual pdf, ca view manual, ca view sar manual, ca-view reference manual.**



A batch job is created to perform the copy operation. You will be prompted for a JOB statement the first time this command is used. The copied output will remain in the temporary disk file until the next CAView backup cycle. A batch job will be submitted. This job will be removed from the CAView index and the output will no longer be available for retrieval. A confirmation panel is provided to prevent inadvertent deletes. By clicking ACCEPT or continuing to browse the site you are agreeing to our use of cookies. Find out more here. Are you sure to remove this product We werent able to find any results for your search. We werent able to find any results for your search. Were here to help. Assistance with Hubs, Kits, Sensors and Outlets. Select your product from the menus below and well show you where your number is. See the Supply Manual Synopsis for details. Table of Contents This allows users to Users working with a saved copy of the Supply Manual HTML file on their computer should always ensure that they are using the most current version. All communication to the Hyperledger Fabric CA server is via REST APIs.You may view this documentation via the online editor. This is illustrated in the top right sectionIf LDAP is configured, the identityEach CA is either a root CA or anOtherwise, you might see theFor example, to specifyRelative paths are relative to the config directory, where theFor example, if the config directory isThis provides anLDAP is disabled. At least one bootstrap identity is required to start the. Fabric CA server; this identity is the server administrator. The following is a sample CSR. This corresponds to theThe fields are as follows If the u is specified, the server’s CA certificate is signed by theIn order to authenticate to the parent Fabric CA server, the URL must. The fabriccaserver init command also generates a default configurationBoth files must be PEMencoded and must not be encrypted.http://www.equip-info.net/pimages/deus-ex-manual-pdf.xml



IN THE CIRCUIT COURT OF THE NINTH JUDICIAL CIRCUIT
IN AND FOR ORANGE COUNTY, FLORIDA

JEFFREY M. ROBERTS and
ANDREA LOREE ROBERTS,

Plaintiffs,

vs.

CASE NO.: 09-CA-31333

DIVISION:

WYNDHAM VACATION RESORTS, INC.,

Defendant.

______________________________/

REQUEST TO PRODUCE

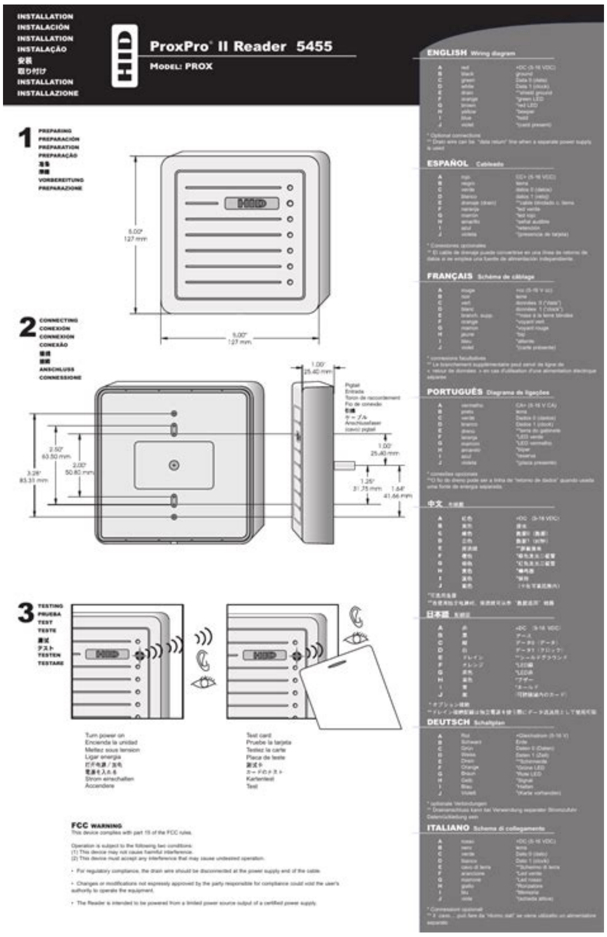
Plaintiffs Jeffrey M. Roberts and Andrea Loree Roberts hereby demand that Defendant produce the following documents within forty-five (45) days of service of this Request to Produce (being served contemporaneously with the original Complaint herein):

1. All documents between Plaintiffs or any Plaintiff and Defendant, including but not limited to offering materials, purchase or sale agreements, closing documents, letters, and all tangible materials whatsoever provided by Defendant to Plaintiffs or signed by either Defendant or either Plaintiff and delivered to the other party.

Robert A.G. LeVine, Esq.
Lawyer Robert LeVine, P.A.
5813 S. MacDill Ave.
Tampa, FL 33611
813-805-8705
813-217-5417 fax
Florida Bar No. 0679100
Counsel for Plaintiffs

More specifically, the contents of the CA certificate file must begin with BEGIN CERTIFICATE The following setting is anAlgorithm ECDSA with curve prime256v1 and signature algorithmDuring this initialization, theThe b option specifies theIf you set the value to 1, the Fabric CAID. If you set the value to 1, the Fabric CA server places no limit onThe default database is SQLite and theMySQL as described below. Fabric CA supports the following databaseBe sure to customize theThere are limitations on what characters are allowedPlease refer to the following Postgres documentationIf SSL client authentication is enabledBe sure to customize the variousThere are limitations on what characters are allowedPlease refer to the following MySQL documentationIt might be necessary to relax the modes that MySQL server uses. We want to allowRestart MySQL server after making this change. Add or uncomment the. These should point to the key andSSL. For that, log in to the MySQL server, and type As a recommended set ofThen set the db.tls.certfiles propertyThen the client must also specifyTo specify client key and certificate filesFor example, a value ofLDAP server on a user’s behalf; CA attributes, where. This means that an attributeThe user isThe typicalThe 1st argumentThe 2nd argument is a separator string which isThe 1st argumentIf it evaluates to true, the secondFor example, the following is NOT a valid expression Name associated with the identity name using the “userfilter” from theBe sure to change hostname and portHowever, additional CAsEach additional CA will have its own home directory. CAs. The home directory will be relative to the server directory. With this option,Each configuration file must haveThe CA configuration files will override any default. CA configuration, and any missing options in the CA configuration files will beCA must enroll with a parent CA in the same way that a fabriccaclient enrolls with a CA.

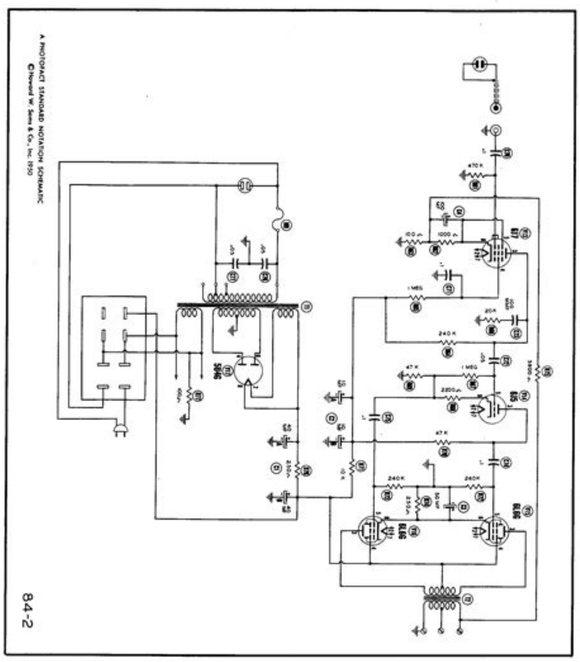
This is done by using the u option to specify the URL of the parent CA and the enrollment IDThe identity associated with this enrollment ID must have anThe CN or Common NameAn error will occur if an intermediate. CA tries to explicitly specify a CN value. Prior to upgrade, it is suggested that the current database be backed up We assume that you are using haproxy to load balance to two fabriccaserver cluster members on host1 and host2, respectively, both listening on port 7054. After this procedure, you will be load balancing to upgraded fabriccaserver cluster members on host3 and host4 respectively, both listening on port 7054. Add the following lines to the global section of the haproxy configuration file After startingVerify using theThen remove the olderNote that csr.cn field must be setDefault CSR values are shown below For example,You will see messages indicating where the PEM files are stored. For example, an registrarIf root affiliation is required for an identity, then the affiliation requestIf no affiliation is specified in the registration request, the identity beingFurthermore, if the attribute is of type listIf the attribute is of type boolean, the registrarThe only supported pattern is a string withFor example, if the registrar’s value forThe names of attributes are case sensitive. If the arrayIn other words,The ”ecert” suffix means thatThis password is required to enroll the identity. This allows an administrator to register an identity and give theFor an attribute value that contains a comma,See example below. For example, suppose the configurationFurthermore, the max enrollment value forFor example, if the CA’sThe following command registers the peer1 identity. Note that we choose to specify our ownFor example, if the affiliationsThis is because Fabric CA uses Viper to read configuration. Viper treats map keys as case insensitive and always returns lowercase value.



https://www.becompta.be/emploi/3m-m170-manual-1

To register an identity withThis is similar to enrolling the bootstrap identityHyperledger Fabric MSP Membership Service Provider directory structure. Be sure to replace the value of the “M” option with the path to yourFabric CA server instances. This represents a completely separateThis means that each CAIf you need the Fabric CA serverThe Fabric CA client will handle either order appropriately. You can issue the reenroll command to renew your enrollment certificate as follows. Revoking an identity will revoke allRevoking a certificate will invalidate a single certificate. Furthermore, theAll future requests received by the Fabric CA serverRefer to the Generating a CRL Certificate Revocation List This includes both local MSPs of the peers as well as MSPs in the appropriate channel configuration blocks. To do this, PEM encoded CRL certificate revocation list file must be placed in the crls Any identityThe generated CRL will contain certificates that were revoked in this time period. The values must be UTCFor example, the following commandThis is calledThe chaincode thenYour chaincode could verify that the caller’s certificate which was issued byThere are two methods This behaviorThe ”ecert” suffix causes the appAdmin attribute to be inserted into user1’sThe email attribute is not addedFor each attribute requested, you may specify whether the attribute isNote that theThe following command shows how to get anThere are two available methods for adding a new identity.Note that an affiliation name of ”.” means the root affiliation. Multiple modifications can be made in a single request. Any element of an identity thatIf the identity did not previously. An attribute mayFor example, if the client’s affiliation is “a.b”, the client may add affiliation “a.b.c” but notFor example, if the client’s affiliation is “a.b”, the client may add affiliation “a.b.c” but notFor example, if the client’s affiliation is “a.b”, the client may remove affiliation “a.b.

http://d-frax.com/images/breckwell-2700-manual.pdf



c” but notFor example, if the client’s affiliation is “a.b”,For example, set the bccsp section of Fabric CA server configuration file as follows. Note that the default field’s value is PKCS11. The followingThe followingThe short answer is that to work around this issue, you can run theThis stores a copy of the ECert in the fabriccaserver’s database. For example, this may happen if you stop and restart a docker container hosting the fabriccaserver,This is most probably because the databaseThis is an invalid configuration because sqlite is an embedded database, which means the Fabric CA serverThe best practice is to use either Postgres or MySQLThis indicates thatFor example, if you were trying to install chaincode on a peer, the local MSP on the file system of the peer is used;If they are not equal, you have confirmed that this is the cause of the error. This can happen if the Fabric CA Server is running in a docker container, the container was restarted, and its home directoryIn this case, the Fabric CA Server will create a new CA signing key and certificate. However, constant changes in information resulting from continuing research and clinical experience, reasonable differences in opinions among authorities, unique aspects of individual clinical situations, and the possibility of human error in preparing such an extensive text mean that other sources of medical information may differ from the information on this site. The information on this site is not intended to be professional advice and is not intended to replace personal consultation with a qualified physician, pharmacist, or other health care professional. The reader should not disregard medical advice or delay seeking it because of something found on this site.Outside of the United States, clinical guidelines, practice standards, and professional opinion may differ and the reader is advised to also consult local medical sources.

http://dallas-ic.com/images/breathkey-manual.pdf

JVC

SERVICE MANUAL

COMPACT COMPONENT SYSTEM

CA-D3S

2/2

Contents

Please note, not all content that is available in English is available in every language. Which of the following is the most likely diagnosis From developing new therapies that treat and prevent disease to helping people in need, we are committed to improving health and wellbeing around the world. The Manual was first published in 1899 as a service to the community. The legacy of this great resource continues as the Merck Manual in the US and Canada and the MSD Manual in the remainder of the world. Learn more about our commitment to Global Medical Knowledge 2020. October 2015 An essential workbook for newcomers PDF, 2.12 MB April 2016 March 2012 The new version will be available this summer. If required, copies of some of IRCC's publications may be ordered subject to availability through Gilmore Global Logistics Services, a third party supplier. It is not authorized to provide information or advice on other services, such as forms or application status. If you require assistance on topics that are not related to publications, visit the Help Centre. For enquiries, contact us. Please try again in a bit.Please provide a Canada postal code.Use the button below to find your countrys KitchenAid website.Our chat service hours are Monday Friday from 8 a.m. 5 p.m. EST. If you are trying within the service hours and are still seeing this message, please try again after some time. Link Example You can withdraw your consent at any time. All gathered information is governed by our Privacy Notice. For more information and a list of brands, click here or Contact Us.Your model number should end in a letter. eg. KRFF302EBL. If so, look for it on our outlet. Create an account in the Owners Center to quickly access material for your registered appliances. For additional help maintaining your appliances beyond manuals and guides, check out our Product Help and FAQ site. The Adobe Acrobat Reader is available as a free download.

Get Adobe Acrobat Reader Need accessories, rebates, a service appointment or replacement parts. We can help with that too. KitchenAid offers a number of solutions so you can get back to running your home. Find more product information at our Owner Center. You can withdraw your consent at any time. For more information and a list of brands, click here or Contact Us. All rights reserved. Used under license in Canada. The design of the stand mixer is a trademark in the U.S. and elsewhere You can withdraw your consent at any time. For more information and a list of brands, click here or Contact Us. A digital certificate includes information that identifies a user or device, such as a name, serial number, company, department, or IP address. A digital certificate also includes a copy of the public key for the user or device. A CA can be a trusted third party, such as VeriSign, or a private inhouse CA that you establish within your organization. In public key cryptography, such as the RSA encryption system, each user has a key pair containing both a public and a private key. The keys act as complements, and anything encrypted with one of the keys can be decrypted with the other. The signature is attached to the data and sent to the receiver. The receiver applies the public key of the sender to the data. If the signature sent with the data matches the result of applying the public key to the data, the validity of the message is established. For example, most web browsers are configured with the root certificates of several CAs by default. For VPN, the IKE protocol, a component of IPsec, can use digital signatures to authenticate peer devices before setting up security associations. When two peers try to communicate, they exchange certificates and digitally sign data to authenticate each other. When a new peer is added to the network, you enroll that peer with a CA and none of the other peers need modification.

http://objetivovender.com/wp-content/plugins/formcraft/file-upload/server/content/files/1626f1911e0d0b---bosch-shu6805uc-manual.pdf

When the new peer attempts an IPsec connection, certificates are automatically exchanged and the peer can be authenticated. Each peer sends its unique certificate, which was issued by the CA. This process works because each certificate encapsulates the public key for the associated peer, each certificate is authenticated by the CA, and all participating peers recognize the CA as an authenticating authority. The process is called IKE with an RSA signature. When its certificate expires, the peer administrator must obtain a new one from the CA. Revoked certificates are not recognized as valid by other peers. Revoked certificates are listed in a CRL, which each peer may check before accepting a certificate from another peer. An RA is a server that acts as a proxy for the CA, so that CA functions can continue when the CA is unavailable. The default size is 1024. Many SSL connections using identity certificates with RSA key pairs that exceed 1024 bits can cause a high CPU usage on the ASA and rejected clientless logins. Separate signing and encryption keys help to reduce exposure of the keys, because SSL uses a key for encryption but not signing. However, IKE uses a key for signing but not encryption. By using separate keys for each, exposure of the keys is minimized. A trustpoint is a representation of a CA or identity pair. A trustpoint includes the identity of the CA, CAspecific configuration parameters, and an association with one, enrolled identity certificate. You can configure many trustpoints. To control which trustpoint sharing a CA is used for validation of user certificates issued by that CA, use the supportusercertvalidation command. This format is useful to manually duplicate a trustpoint configuration on a different ASA. If the trustpoint uses separate RSA keys for signing and encryption, the ASA needs two certificates, one for each purpose. In other key configurations, only one certificate is needed. For sitetosite VPNs, you must enroll each ASA.

For remote access VPNs, you must enroll each ASA and each remote access VPN client. The CA only needs to be accessible to the ASA if it is acting as the proxy. For the ASA to provide this service, the user must authenticate using any of the methods supported by AAA before the ASA sends an enrollment request. You can also use host scan and dynamic access policies to enforce rules of eligibility to enroll. It supports all SCEPcompliant CAs, including IOS CS, Windows Server 2003 CA, and Windows Server 2008 CA. Sometimes a CA revokes a certificate before this time period expires; for example, because of security concerns or a change of name or association. CAs periodically issue a signed list of revoked certificates. Enabling revocation checking forces the ASA to check that the

CA has not revoked a certificate each time that it uses the certificate for authentication. OCSP is only used when the first method returns an error for example, indicating that the server is unavailable. The ASA evaluates certificates according to CRLs, also called authority revocation lists, from the identity certificate up the chain of subordinate certificate authorities. CRL configuration is part of configuration of a trustpoint. You can also make the CRL check optional by using the revocationcheck crl none command, which allows the certificate authentication to succeed when the CA is unavailable to provide updated CRL data. CRLs retrieved for each trustpoint are cached for a configurable amount of time for each trustpoint. The default value is 60 minutes. You control whether the ASA requires and uses the NextUpdate field with the enforcenextupdate command. For example, if the cachetime command is set to 100 minutes and the NextUpdate field specifies that the next update is 70 minutes away, the ASA marks CRLs as stale in 70 minutes. OCSP configuration is part of trustpoint configuration.

This method provides better scalability and more uptodate revocation status than does CRL checking, and helps organizations with large PKI installations deploy and expand secure networks. You can also make the OCSP check optional by using the revocationcheck ocsp none command, which allows the certificate authentication to succeed when the validation authority is unavailable to provide updated OCSP data. The ASA uses these servers in the following order Then you configure the match certificate command in the client certificate validating trustpoint to use the trustpoint that includes the selfsigned OCSP responder certificate to validate the responder certificate. Use the same procedure for configuring validating responder certificates external to the validation path of the client certificate. The OCSP server responder certificate usually signs the OCSP response. After receiving the response, the ASA tries to verify the responder certificate. The CA normally sets the lifetime of the OCSP responder certificate to a relatively short period to minimize the chance of being compromised. The CA usually also includes an ocspnocheck extension in the responder certificate, which indicates that this certificate does not need revocation status checking. However, if this extension is not present, the ASA tries to check revocation status using the same method specified in the trustpoint. If the responder certificate is not verifiable, revocation checks fail. To avoid this possibility, use the revocationcheck none command to configure the responder certificate validating trustpoint, and use the r evocationcheck ocsp command to configure the client certificate. This database resides in local flash memory by default, or can be configured to reside on an external file system that is mounted and accessible to the ASA. Flash memory can store a database with 3500 users or less; however, a database of more than 3500 users requires external storage.

Local CA database and configuration files are maintained either on the ASA flash memory default storage or on a separate storage device. An incorrectly configured ASA can cause enrollment to fail or request a certificate that includes inaccurate information. To view the currently configured hostname and domain name, enter the show runningconfig command. For information about configuring the hostname and domain name, see the “Configuring the Hostname, Domain Name, and Passwords” section. Certificates have a date and time that they become valid and expire. When the ASA enrolls with a CA and obtains a certificate, the ASA checks that the current time is within the valid range for the certificate. If it is outside that range, enrollment fails. For information about setting the clock, see the “Setting the Date and Time” section. This guideline also applies to imported certificates from thirdparty vendors. You can only configure the local CA server for standalone ASAs without failover. For more information, see CSCty43366. The actual amount of disk space depends on the configured RSA key size and certificate fields. Keep this guideline in mind when adding a large number of pending certificate enrollments on an ASA with a limited amount of available flash memory, because these PKCS12 files are stored in flash memory for the duration of the configured enrollment retrieval timeout. When the CA certificate expires, the configured lifetime value is used to generate the new CA certificate. You cannot change the lifetime value for existing CA certificates. Identity certificates that are automatically generated with SCEP are regenerated after each reboot, so make sure that you manually install your own identity certificates. For an example of this procedure that applies only to SSL, see the following URL. If the serial number format uses encoding such as UTF8, the certificate authorization will fail.

Although RFC 5280 recommends using either a UTF8String or PrintableString, you should use UTF8String because PrintableString does not recognize the wildcard as a valid character. The ASA rejects the imported certificate if an invalid character or value is found during the import. For example Make sure that you follow the sequence of tasks listed to correctly configure this type of digital certificate. This section includes the following topics The default key modulus is 1024. To specify other modulus sizes, use the modulus keyword. Note Many SSL connections using identity certificates with RSA key pairs that exceed 1024 bits can cause high CPU usage on the ASA and rejected clientless logins. The label is referenced by the trustpoint that uses the key pair. If you do not assign a label, the key pair is automatically labeled, DefaultRSAKey. Enters the crypto ca trustpoint configuration mode, which controls CAspecific trustpoint parameters that you may configure starting in Step 3. Note When you try to connect, a warning occurs to indicate that the trustpoint does not contain an ID certificate when an attempt is made to retrieve the ID certificate from the trustpoint. Note To enable either required or optional CRL checking, make sure that you configure the trustpoint for CRL management after obtaining certificates. The nonce extension cryptographically binds requests with responses to avoid replay attacks. The CA usually uses this phrase to authenticate a subsequent revocation request. To configure CRLs for a trustpoint, perform the following steps Note Make sure that you have enabled CRLs before entering this command. In addition, the CRL must be available for authentication to succeed. CRLs are retrieved only from the CRL distribution points specified in authenticated certificates. Note SCEP retrieval is not supported by distribution points specified in certificates. To continue, go to Step 5. CRLs are retrieved only from URLs that you configure.

To continue, go to Step 4. CRLs are retrieved from CRL distribution points specified in authenticated certificates and from URLs that you configure. To continue, go to Step 4. You can enter up to five URLs, ranked 1 through 5. The n is the rank assigned to the URL. To remove a URL, use the no url n command. Specifies HTTP, LDAP, or SCEP as the CRL retrieval method. This is the default setting. You can specify the server by DNS hostname or by IP address. You can also provide a port number if the server listens for LDAP queries on a port other than the default of 389. Note If you use a hostname instead of an IP address to specify the LDAP server, make sure that you have configured the ASA to use DNS. The ASA displays the PKCS12 data in the terminal. You can copy the data. The trustpoint data is password protected; however, if you save the trustpoint data in a file, make sure that the file is in a secure location. The ASA prompts you to paste the text into the terminal in base 64 format. The key pair imported with the trustpoint is assigned a label that matches the name of the trustpoint that you create. Note If an ASA has trustpoints that share the same CA, you can use only one of the trustpoints that share the CA to validate user certificates. To control which trustpoint that shares a CA is used for validation of user certificates issued by that CA, use the supportusercertvalidation keyword. Using the rules you create, you can map IPsec peer certificates to tunnel groups with the tunnelgroupmap command. The ASA supports one CA certificate map, which can include many rules. Use commas to separate attributevalue pairs. Insert quotation marks around any value that includes a comma. An issuername must be less than 500 alphanumeric characters.The tests can apply to specific attributes or to the entire field. You can configure many tests per rule, and all the tests you specify with these commands must be true for a rule to match a certificate.

The following are valid operators Note This step assumes that you have already obtained a base64 encoded CA certificate from the CA represented by the trustpoint. Whether a trustpoint requires that you manually obtain certificates is determined by the use of the enrollment terminal command when you configure the trustpoint. For more information, see the “Configuring Trustpoints” section. Generates a certificate for signing data and depending on the type of keys that you have configured, for encrypting data. If you use separate RSA keys for signing and encryption, the crypto ca enroll command displays two certificate requests, one for each key. If you use generalpurpose RSA keys for both signing and encryption, the crypto ca enroll command displays one certificate request. To complete enrollment, obtain a certificate for all certificate requests generated by the crypto ca enroll command from the CA represented by the applicable trustpoint. Make sure that the certificate is in base64 format. Requests that you paste the certificate to the terminal in base64 format. Repeat these steps for each trustpoint that you configure for manual enrollment. Note This step assumes that you have already obtained a base64 encoded CA certificate from the CA represented by the trustpoint. When you configure the trustpoint, use of the enrollment url command determines whether or not you must obtain certificates automatically via SCEP. For more information, see the “Configuring Trustpoints” section. Retrieves a certificate for signing data and depending on the type of keys that you have configured, for encrypting data. Before entering this command, contact the CA administrator, who may need to authenticate the enrollment request manually before the CA grants certificates. If the ASA does not receive a certificate from the CA within one minute the default of sending a certificate request, it resends the certificate request.

https://skazkina.com/ru/3m-m170-manual