Johnson Controls

P2000AE

Security Management System

Encryption Configuration

for Communicating with CK722 Panels

Version 4.1 and higher, December, 2008
24-10241-135 Revision B

(805) 522-5555
www.johnsoncontrols.com

These instructions are supplemental. Often they are supplemental to other manufacturer's documentation. Never discard other manufacturer's documentation. Publications from Johnson Controls, Inc. are not intended to duplicate nor replace other manufacturer's documentation.

If this document is translated from the original English version by Johnson Controls, Inc., all reasonable endeavors will be used to ensure the accuracy of translation. Johnson Controls, Inc. shall not be liable for any translation errors contained herein or for incidental or consequential damages in connection with the furnishing or use of this translated material.

ENCRYPTION CONFIGURATION FOR CK722 PANELS

If you use the P2000AE system with CK722 controllers, you can provide an additional measure of security for your communications by using encryption. Without encryption, someone with access to your network could conceivably view or change your configuration, access privileges, events, and so on, thereby compromising system security.

To use encryption with the P2000AE software, you must edit settings in the Windows® operating system. The following sections describe how to enable encryption on the P2000AE server computer communicating with CK722 controllers.

NOTE

- *The screen captures shown in this manual may differ slightly, depending on the P2000 software version you are using.*
- *The instructions in this manual were written using Microsoft Windows Server 2003 operating system. Some Windows configuration steps may vary, depending on your operating system and whether or not you use CDs or a DVD to install Windows.*
- *"P2000AE" is also referred to as "P2000" throughout this manual.*

GETTING STARTED

Prepare for Installation

To perform the following sequence of steps, be ready to do the following:

- Have your original installation CD for your Windows operating system available. You will be prompted to add files from the CD.
- Installation assumes that you have at least one CK722 controller installed, configured, and operating on your system.
- Shut-down the P2000 system and all Windows programs, including the P2000 Service Monitor.

Sequence of Steps

Once the P2000 software is installed at the server and the CK722 controllers are configured, you will be ready to begin the Certificate of Authority installation. You will perform the following sequence of steps:

- **Install the Certificate of Authority**
- **Configure P2000 for Encryption**
- **Enable Controller Encryption**
- **Approve Certificate Requests, if required.**
- **Revoke Previously Issued Certificates**

Detailed instructions to perform each step are presented in the following sections.

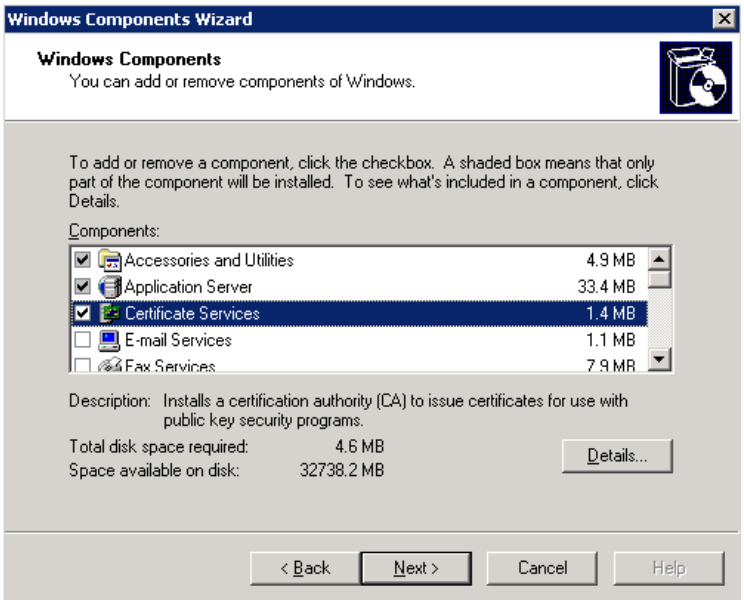
INSTALL CERTIFICATE OF AUTHORITY

NOTE

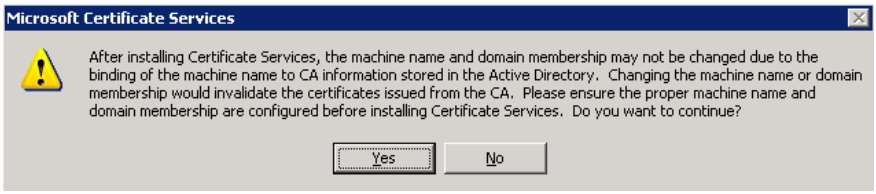
During this step, you will be prompted to insert your original Windows operating system CD. Be sure to have it ready.

➤ To Install Certificate of Authority:

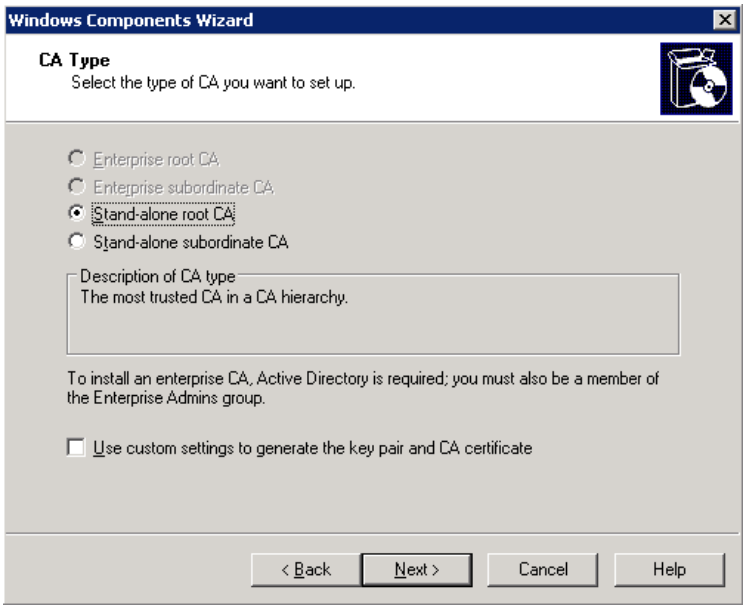
1. Shut-down the P2000 system and all Windows programs, including the P2000 Service Monitor.
2. On the Windows Server desktop, go to **Start>Settings>Control Panel**.
3. Open **Add or Remove Programs**.
4. Click the **Add/Remove Windows Components** icon in the column on the left side of the window. The Windows Components Wizard opens.



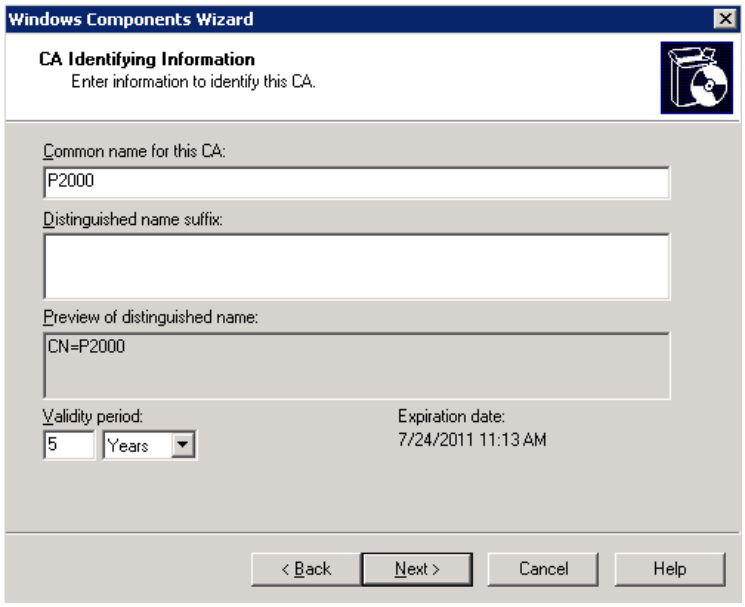
5. Select **Certificate Services**. The following warning will display:



6. Read the warning as it is important to future system operation. Click **Yes** to continue.
7. In the Windows Components Wizard, click **Next** to continue. The CA Type dialog box opens.



8. Ensure **Stand-alone root CA** is selected and click **Next** to continue. The CA Identifying Information dialog box opens.

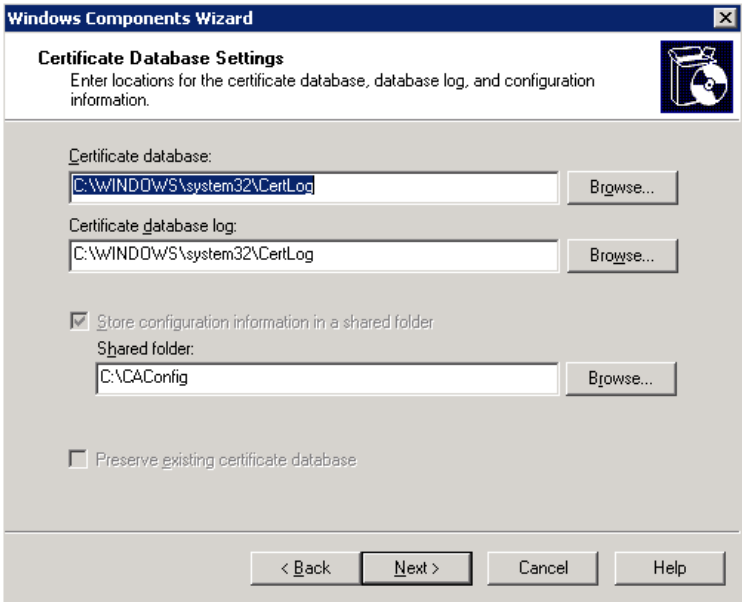


9. In the **Common Name for this CA** box, type in a name, such as P2000. This value must be the same as the Certificate Authority value in the General tab of Site Parameters, see page 8.
10. Assign a **Validity period**. We recommend the default of five years.

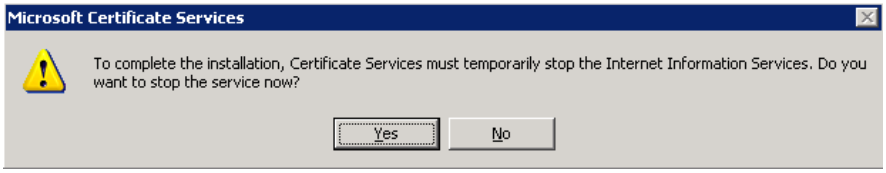
NOTE

The default is five years. If you reduce it to one year, you will have to get another certificate of authority at that time. Five years is a reasonable selection.

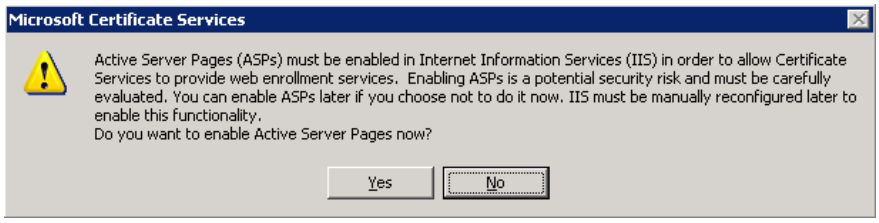
11. Click **Next** to continue. The Certificate Database Settings dialog box opens.



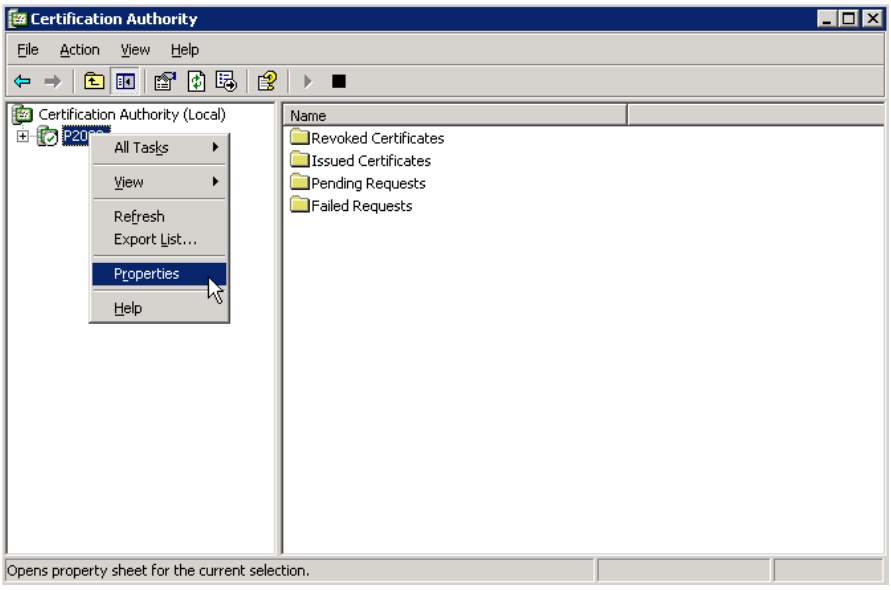
12. Unless you have a specific need to change the database locations, we recommend you accept the default locations. Click **Next** to continue. You will see the following warning:



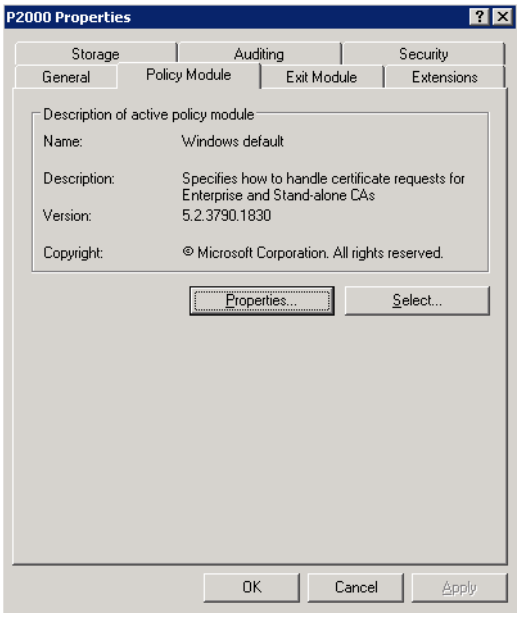
13. Click **Yes** to continue. The system will configure the components. During this process, you will be asked to insert your Windows Server 2003 CD-ROM.
14. Insert the CD-ROM and click **OK**. The program will continue configuring files. The following warning will appear:



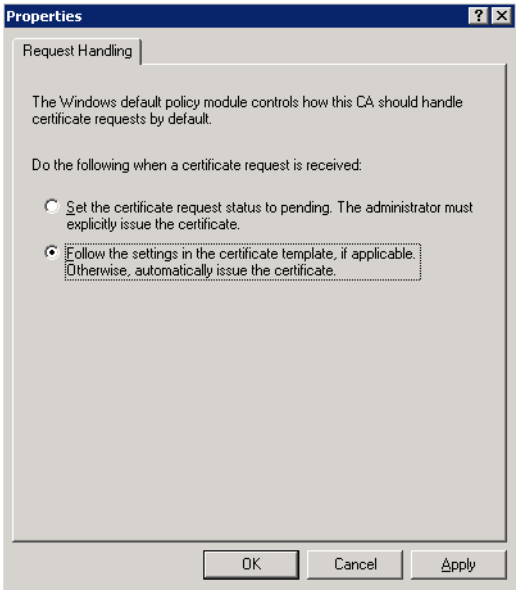
15. Unless you have a specific need for this operation, click **No**.
16. Click **Finish** when Windows Components Wizard completes the process.
17. Close **Add or Remove Programs** to return to the Control Panel.
18. In the Control Panel, select **Administrative Tools** and double-click the **Certification Authority** icon. The Certification Authority window opens.



19. Right-click the newly created CA and select **Properties**. The Properties dialog box opens. Click the **Policy Module** tab.



20. Click the **Properties** button to open the Request Handling tab.



21. If you wish to configure the CA to automatically approve certificate requests, select the **Follow the settings in the certificate template, if applicable. Otherwise, automatically issue the certificate** option.
22. If you select the **Set the certificate request status to pending. The administrator must explicitly issue the certificate** option, all certificate requests to this CA will be considered "pending" and the administrator will have to manually approve or reject the requests. Refer to "Approve Certificate Requests" on page 13 for instructions.

23. Click **OK** to close the Request Handling tab.
24. A message displays to restart Certificate Services for the changes to take effect, click **OK**.
25. Click **OK** to close the Properties dialog box.
26. Right-click the CA name and select **All Tasks>Stop Service**. Once the service is stopped, right-click the CA name again and select **All Tasks>Start Service**.
27. Close all windows, remove the CD-ROM and **Reboot**. When the system comes back up, you are ready to proceed to the next section.

CONFIGURE P2000 FOR ENCRYPTION

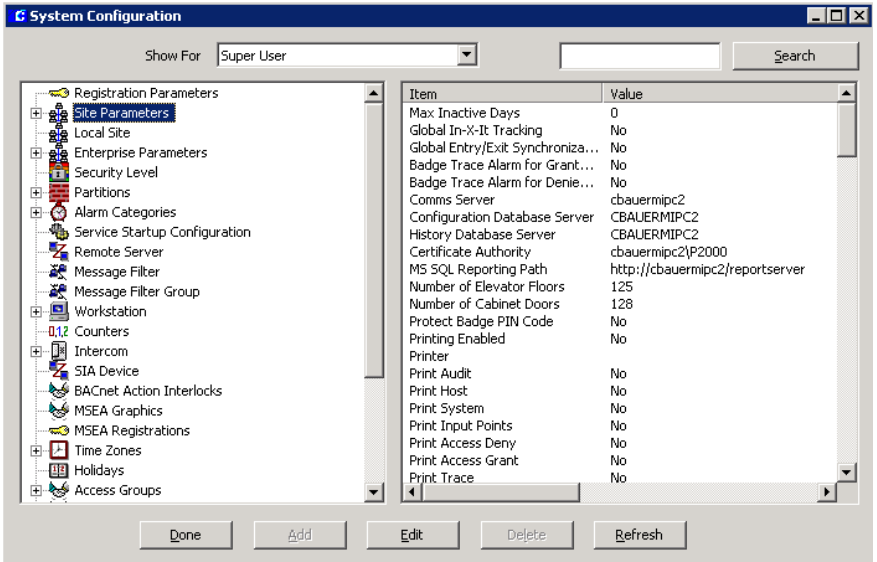
You must configure the P2000 software to allow encryption between the CK722 panels and the P2000 Server.

NOTE

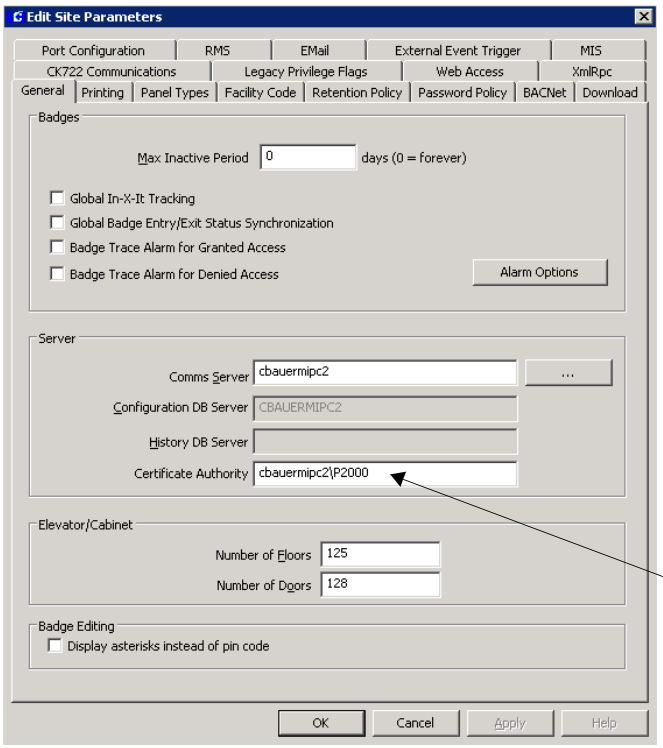
Once you change the settings described in the following steps, they must NEVER change.

➤ **To Configure P2000 for Encryption:**

1. Launch P2000.
2. From the P2000 Main menu, select **Config>System**. The System Configuration window opens.



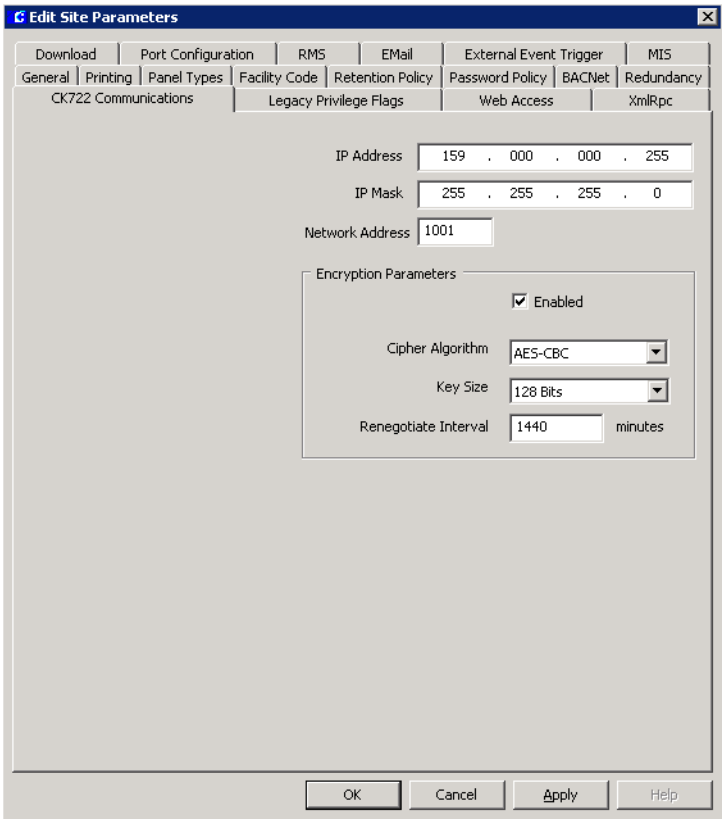
3. Select **Site Parameters** and click the **Edit** button at the bottom of the window. The **Edit Site Parameters** dialog box opens displaying the General tab.



4. Make sure the **Certificate Authority** field displays the certificate name previously defined on page 4. If it is not the same, enter the correct name here.
5. Select the **CK722 Communications** tab.

NOTE

Settings in this tab are required to communicate with CK722 panels.



The following fields should already be defined and indicate:

- The **IP Address** of the object engine that is used to communicate with CK722 panels.
- The **IP Mask** address of the object engine.
- The **Network Address** default value.

6. In the Encryption Parameters box, select **Enabled** to allow encryption of all messaging between CK722 panels and the P2000 Server.
7. Select the **Cipher Algorithm** type you wish to use. See the following descriptions for more information about algorithm types:
   - **AES-CBC** – Advanced Encryption Standard. Strong encryption with long expected life. Key sizes: 128, 192, and 256 bits.
   - **3DES-CBC** – DES repeated three times. Provides strong protection. Key size: 192.
   - **DES-CBC** – Lower level security. Key size: 64.

NOTE

For more information about encryption standards refer to www.nist.gov.

8. If you selected AES, select the **Key Size** you wish to use. The greater the key number the higher the security, however the panel communications could be slower.
9. Enter a **Renegotiate Interval**. Periodic renegotiation refreshes the keys to limit the time a key is exposed. We recommend you use the default.
10. Click **OK**.
11. **Close** the System Configuration window.
12. **Reboot** the system. When the system comes back up, you are ready to proceed to the next section.

    If the CA was configured for manual approval, see "Approve Certificate Requests" on page 13 for details.

NOTE

*The **P2000 Certificate Service** must be running at the P2000 Server to provide an interface between the CK722 controllers and Microsoft Certificate Authority. The CK722 sends certificate requests to the P2000 Certificate Service, the P2000 Certificate Service sends the request to Microsoft Certificate Authority, and when the reply comes back, the P2000 Certificate Service sends it to the CK722. Refer to the P2000 Software User Manual for instructions.*

ENABLE CONTROLLER ENCRYPTION

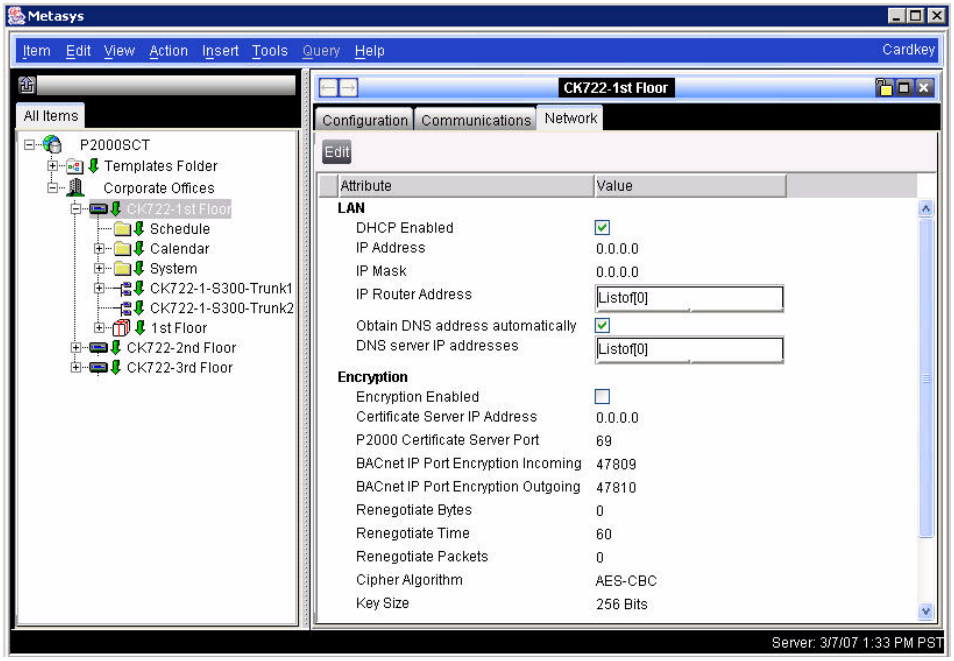
Once you have completed P2000 configuration to allow for encryption, you must enable controller encryption. Launch P2000 to perform the following steps.

➤ To Enable Controller Encryption:

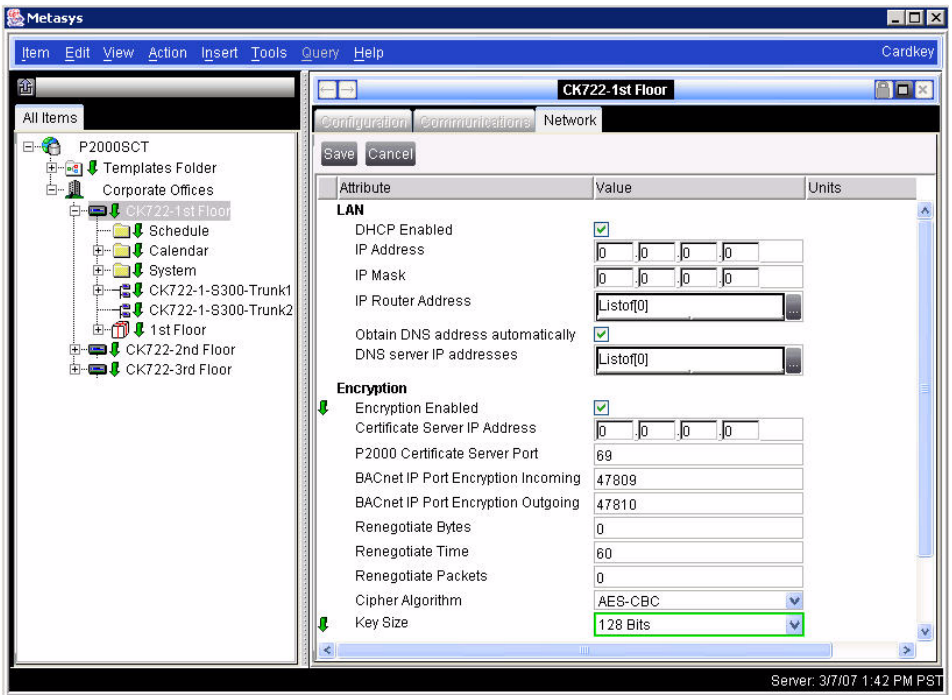
1. Launch P2000.
2. From the P2000 Main menu, select **Config>SCT**. The System Configuration Tool program takes a moment to load.
3. In the Navigation Tree frame (left pane), drill down through the node tree to select the site and controller you wish to enable for encryption.
4. Double-click on the controller.

NOTE

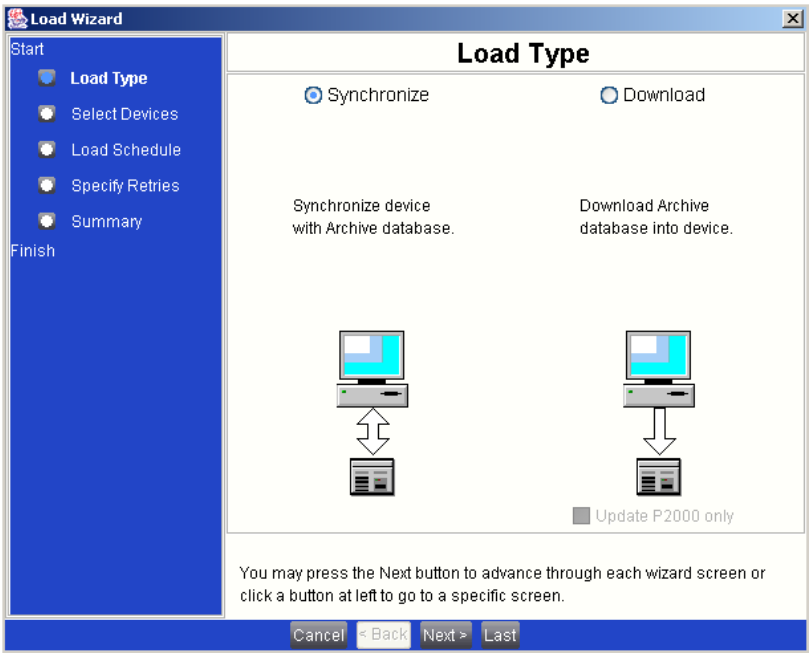
*Before you enable encryption for the selected controller, open the Database Maintenance application from the P2000 Main menu bar and run the **CK722 Maintenance Start** task to take the selected controller offline from the P2000 Server. In addition, open the P2000 **Real Time List** and verify the transactions as they occur. Refer to the P2000 Software User Manual for instructions.*



5. Select the **Network** tab, then click the **Edit** button at the top of the right display.



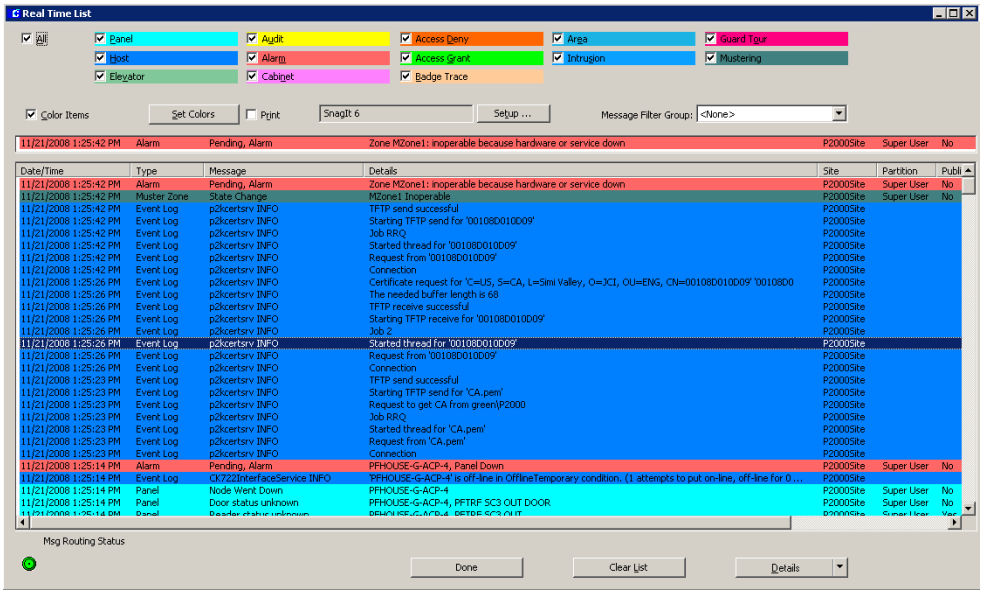
6. Under the Encryption category, select the **Encryption Enabled** check box. Set the remaining parameters per your system setup. The Certificate Server IP Address should be the IP address of the P2000 Server.
7. Click **Save**.
8. From the System Configuration Tool menu bar, select **Tools>Load Archive**. The Load Wizard opens.



9. In the Load Type section, ensure **Synchronize** is selected and click **Next**.
10. Under Select Devices, highlight the controller you want to synchronize and click **Last**. The Summary page will display the controller that will be synchronized.
11. If the information is correct, click **Finish**. The program will take a few minutes to perform the synchronization.

NOTE

*After the synchronization is completed, open the Database Maintenance application from the P2000 Main menu bar and run the **CK722 Maintenance End** task to put the selected controller back online. Verify that the P2000 Real Time List displays the related transaction messages.*



If the CA was configured for manual approval, refer to the following section, “Approve Certificate Requests” for further instructions.

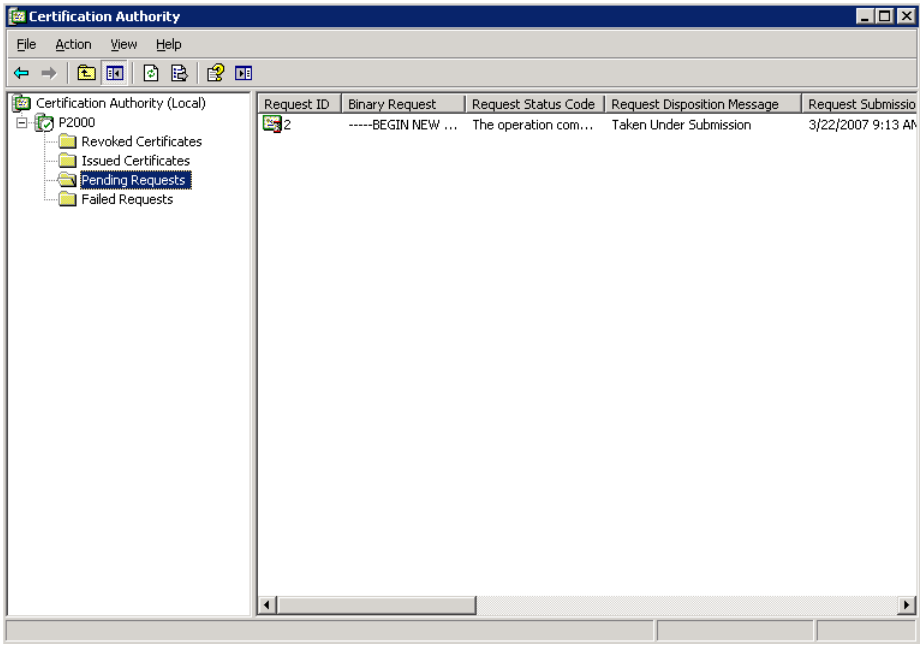
APPROVE CERTIFICATE REQUESTS

If a CA is configured for manual approval (steps 18 to 27, starting on page 5), all incoming certificate requests to the CA will be considered “pending” and will be placed in a Pending folder in the Certification Authority window. The system administrator will have to review the request and decide whether to issue the certificate or reject the request.

➤ To Manually Issue Certificate Requests:

1. On the Windows Server desktop, go to **Start>Settings>Control Panel**.
2. Double-click the **Administrative Tools** icon.

3. In the Administrative Tools window, double-click the **Certification Authority** icon. The Certification Authority window opens.
4. Double-click the CA name to display its folders, then click the **Pending Requests** folder.



5. In the details pane, examine the certificate request by verifying the values for Requester Name, Request Common Name, and any other fields that you consider critical information for issuing the certificate.

NOTE

The Request Common Name field displays the name of the P2000 Server or serial number of the CK722 controller.

6. If you wish to approve the certificate, right-click the certificate request and on the action menu, select **All Tasks**, then click **Issue**.
7. If you wish to reject the certificate, right-click the certificate request and on the action menu, select **All Tasks**, click **Deny**, and then click **Yes**.
8. To verify the certificates that have been issued, click the **Issued Certificates** folder. The details pane will display all issued certificates.
9. Close all windows.

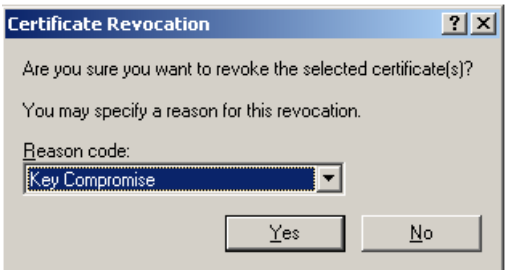
REVOKE PREVIOUSLY ISSUED CERTIFICATES

The administrator of a CA can revoke any certificate at any time if the administrator believes that security has been compromised, or if some other event dictates that a certificate should no longer be considered "valid," such as when a controller's functionality is restored using the Network Utility Tool (NUT).

When a certificate is revoked, it is added to the CA's certificate revocation list (CRL), which lists all certificates issued by the CA that are no longer valid. The CRL is sent to the controllers once every day at midnight. Controllers whose certificates have been revoked, cannot communicate with any other node or P2000 system. When a controller detects that its certificate has been revoked, it eliminates its old set of keys and certificates, and then generates a new set of keys to send a request to obtain a new certificate.

➤ To Revoke an Issued Certificate:

1. On the Windows Server desktop, go to **Start>Settings>Control Panel**.
2. Double-click the **Administrative Tools** icon.
3. In the Administrative Tools window, double-click the **Certification Authority** icon. The Certification Authority window opens.
4. Double-click the CA name to display its folders, then click the **Issued Certificates** folder.
5. In the details pane, right-click the certificate you wish to revoke.
6. On the action menu, select **All Tasks**, then click **Revoke Certificate**. The Certificate Revocation dialog box opens.



7. Select from the **Reason code** drop-down list the reason for revoking the certificate, then click **Yes**.

   The certificate will display in the details pane when you click the **Revoked Certificates** folder. For detailed information on how to manually publish and/or schedule the publication of a CRL, refer to your Microsoft documentation.