ektron

What do you want your website to do?

Ektron CMS400.NET eCommerce Module Implementation Guide for PCI DSS Compliance

ektron CMS400.net

Version 1.3
Created On: 07/21/2009

Revision History			
Revision 1.0	02/17/2009	Steven Hughes	Initial release for compliance review.
Revision 1.1	05/01/2009	Steven Hughes	Rearranged information and updated several areas of the book based on feedback from the compliance auditing team.
Revision 1.2	05/22/2009	Steven Hughes	Added section for updating supporting software. Added documentation location, update CMS400.NET, and review info to “Introduction” section. Added note about using AES for password encryption to appropriate sections. Added that payment options and default gateway information is logged when changed. Added path to the login page.
Revision 1.3	07/21/2009	Steven Hughes	Added new Enable Compliance dialog box description and information to the “Steps to Install the CMS400.NET Min Site” section. Added “Disable HTTP TRACE/TRACK in Microsoft IIS” and “Do Not Allow the Use of the SSL 2.0 Protocol on the Server” sections. Updated information on “Allow connections only from specific known IP and/or MAC addresses.” Added section “Never Allow the Use of Live Cardholder Data or Personal Account Numbers for Development, Testing or Troubleshooting.” Added section “Use HTTP or HTTPS Protocols and Service Ports.”

Table of Contents

1 Introduction

This document is required as part of Payment Application Data Security Standard (PA DSS) certification as defined by the Payment Card Industry Security Standards Council (PCI SSC).
It is to be used by Ektron CMS400.NET's eCommerce partners and customers to help them implement a secure Web site according to the Payment Card Industry Data Security Standard (PCI DSS).

This guide is divided into three major sections. The first, this section, is an introduction to PCI Compliance. The second section contains a more in-depth look at the PCI DSS payment application environment requirements and how Ektron CMS400.NET meets those requirements. The third section explains how to set up and configure CMS400.NET so it can be used in a PCI DSS compliant environment.

Ektron, Inc. reviews this document annually, whenever the CMS400.NET eCommerce module is updated, and whenever updates are made to the Payment Application Data Security Standard.

This guide is added to your server during the CMS400.NET installation. It can be accessed by clicking **Start** > **Programs** > **Ektron** > **CMS400v*Xx*** > **Documentation** > **PA DSS Security Guide**.
For the latest version, see PA-DSS Security Guide.

Ektron CMS400.NET version 7.6.6 is currently in the process of becoming PA DSS certified. Ektron is using an independent PCI SSC approved auditing firm.

Below is a list of CMS400.NET versions supported by this document:

- Ektron CMS400.NET Version 7.6.6

Important! Make sure you apply the latest updates and security patches for CMS400.NET. To check for the latest security updates, see Product Updates. **Note**: You must log into the site to see the available updates. If you are not a registered Dev Center user, click here to register.

1.1 PCI SSC Reference Documents

The following documents detail information about PCI data security and related materials; for example, PCI DSS and PA DSS.

- https://www.pcisecuritystandards.org. This site includes information on:
  - PCI Quick Reference Guide
    - https://www.pcisecuritystandards.org/pdfs/pci_ssc_quick_guide.pdf
  - The PA Data Security Standard
    - https://www.pcisecuritystandards.org/security_standards/pci_pa_dss.shtml
  - The PCI Data Security Standard
    - https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml

Text from these documents appears in certain areas of this document. This text is Copyright 2008 PCI Security Standards Council LLC.

1.2 Who is the PCI Security Standards Council?

From their About Us page:
https://www.pcisecuritystandards.org/about/index.shtml

> *The PCI Security Standards Council is an open global forum, launched in 2006, that is responsible for the development, management, education, and awareness of the PCI Security Standards,*

> *including: the Data Security Standard (DSS), Payment Application Data Security Standard (PA DSS), and Pin-Entry Device (PED) Requirements.*

1.3 What is PA DSS and Why is it Important that Ektron CMS400.NET is Certified?

PA DSS is a certification for software applications that store, process or transmit credit card data during a transaction. Most payment card brands encourage merchants to use payment applications that are certified PA DSS Compliant.

Due to Ektron's leadership position in Content Management and its commitment to security, CMS400.NET is being certified PA DSS to ensure our application conforms to payment card industry standards.

1.4 PA DSS vs. PCI DSS – When Implementing a CMS400.NET Site, Which Certification Do I Need?

It is Ektron's responsibility to become PA DSS certified. In other words, make sure that CMS400.NET is designed in such a way as to meet the standard for payment applications as set by the PCI Security Standards Council.

It is your responsibility to become PCI DSS certified. As a merchant or eCommerce Web site owner, it will be your responsibility to make sure your Web site is PCI DSS Certified. Section 1.5 of this manual provides a high level overview of what it takes to be PCI DSS compliant. For complete information on PCI-DSS compliance, see the PCI DSS document at https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml. You can use the information from that document and the information in this manual to create an Ektron CMS400.NET site that is PCI DSS compliant.

1.5 The Payment Card Industry Data Security Standard

From the PCI Data Security Standard document:

> *The Payment Card Industry (PCI) Data Security Standard (DSS) was developed to encourage and enhance cardholder data security and facilitate the broad adoption of consistent data security measures globally.*

It is your responsibility to become PCI DSS certified. This section talks about the high level concepts you need to implement when obtaining that certification. A lot of this standard revolves around the concepts of storing and maintaining cardholder data. **Ektron CMS400.NET does not store cardholder data.** Because CMS400.NET only passes cardholder data to a payment gateway and does not store it in the application, the standard should be easier for you to meet.

Below are the 12 high level requirements for being PCI DSS compliant.

Goals	PCI DSS Requirement
Build and Maintain a Secure Network	1. Install and maintain a firewall configuration to protect data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect Stored Data 4. Encrypt transmission of cardholder data and sensitive information across public networks
Maintain a Vulnerability Management Program	5. Use and regularly update anti-virus software 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to data by business need-to-know 8. Assign a unique ID to each person with computer access 9. Restrict physical access to cardholder data

Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security

The following documents explain the PCI Data Security Standard:

- For a quick overview, use the PCI Quick Reference Guide
  - https://www.pcisecuritystandards.org/pdfs/pci_ssc_quick_guide.pdf
- For full details, use the PCI DSS
  - https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml

1.5.1 Summary List of How Ektron CMS400.NET Supports PCI DSS Compliance

- Ektron CMS400.NET does not store any customer's credit card data or other sensitive cardholder data. This includes credit card account numbers, expiration dates, checking account and routing numbers, PINs and validation codes.
- Customer's cardholder data is passed through your server to a specified payment gateway via SSL encryption. When your Web site uses SSL, card holder data is encrypted from their browser and sent to your servers. Your server then passes the encrypted data through to your payment gateway provider via an SSL encrypted Web service.
- CMS400.NET does not store card holder data; therefore, there is no card holder data to be removed during the upgrade process.
- Administrators or users with the Commerce Admin role are the only people who can access the eCommerce feature in the CMS400.NET Workarea. The Commerce Admin role allows you to selectively grant eCommerce access to your users without having to make them full administrators.
- CMS400.NET allows you to create unique individual accounts for each user. Each user that interacts with the eCommerce feature is required to have a password that meets PCI-DSS standards. For example:
  - By default, CMS400.NET forces Administrator and Commerce Admin account passwords to be changed at least every ninety days
  - By default, CMS400.NET forces Administrator and Commerce Admin passwords to be at least seven characters long
  - By default, CMS400.NET forces Administrator and Commerce Admin passwords to contain both numeric and alphabetic characters
  - By default, CMS400.NET forces Administrator and Commerce Admin to have passwords that cannot match any of the last four passwords
- Ektron CMS400.NET maintains eCommerce activity logs that document the following types of information:
  - Each time user rights and passwords are changed for administrators or users with the Commerce Admin role.
  - Actions affecting order information, such as updates to an order's address, order transaction ID, actions conducted with the payment gateway and Workflow activities.
  - Login and logout for information for administrator and users with eCommerce Admin role.
- Ektron does not support the use of wireless networking for eCommerce purposes. If you use CMS400.NET in a wireless payment environment, Ektron's PA DSS certification will not apply.
- Email and other end user messaging technologies are never and should never be used to transmit card holder data.
- Ektron CMS400.NET does not allow administrators or users with the Commerce Admin role to view a card holder's data.

2 Payment Application Environment Requirements

This section breaks down different PA DSS and PCI DSS requirements Ektron CMS400.NET needs to meet to become a PA DSS compliant application.

Important! Ektron CMS400.NET does not store cardholder information. It has never stored cardholder data in any previous version. Ektron strongly recommends that you do not store any cardholder data. If you decide to create a way to store customers' credit card data, Ektron's PA-DSS certification will not apply.

Because Ektron CMS400.NET does not store cardholder data and never has in any previous versions, the following PA DSS requirements are not applicable.

- **PA DSS Requirement 1.1.4** - Delete sensitive authentication data stored by previous payment application versions. This section of the requirement states that sensitive historical data (credit card numbers, PINs, etc.) must be removed when upgrading from a previous version of Ektron CMS400.NET.
  - Previous versions of Ektron CMS400.NET have never stored any type of cardholder data.
  - If you are moving to Ektron CMS400.NET from other software that does store this type of information, it needs to be removed for PCI DSS certification.
- **PA DSS Requirement 1.1.5** - Delete any sensitive authentication data (pre-authorization) gathered as a result of troubleshooting the payment application. This section of the requirement states that when troubleshooting the application, sensitive data must only be collected when needed to solve a problem. The data must be encrypted and stored in specific locations, with limited access and must be deleted immediately after use.
  - Ektron CMS400.NET does not store any cardholder data.
- **PA DSS Requirement 2.1** - Purge cardholder data after customer-defined retention period. This section of the requirement states that cardholder data must be removed after the customer-defined retention period.
  - Ektron CMS400.NET does not store any cardholder data.
- **PA DSS Requirement 2.7** - Delete cryptographic key material or cryptograms stored by previous payment application versions. This section of the requirement states that keys from previous versions used to encrypt cardholder data must be removed and the procedure for installing and using new keys must be explained.
  - Because Ektron CMS400.NET does not store cardholder data, it does not use encryption keys; therefore, an explanation is not necessary.
- **PA DSS Requirement 9.1** - Store cardholder data only on servers **not** connected to the Internet. This section of the requirement states that cardholder data cannot be stored on servers that connect to the Internet.
  - Ektron CMS400.NET does not store any cardholder data.
- **PA DSS Requirement 12.2** - Encrypt cardholder data sent over various messaging technologies. This section of the requirement states that when sending cardholder data through end user messaging technologies, such as email, that the data be encrypted.
  - Ektron CMS400.NET does not send cardholder data through email or any other end user messaging technologies.

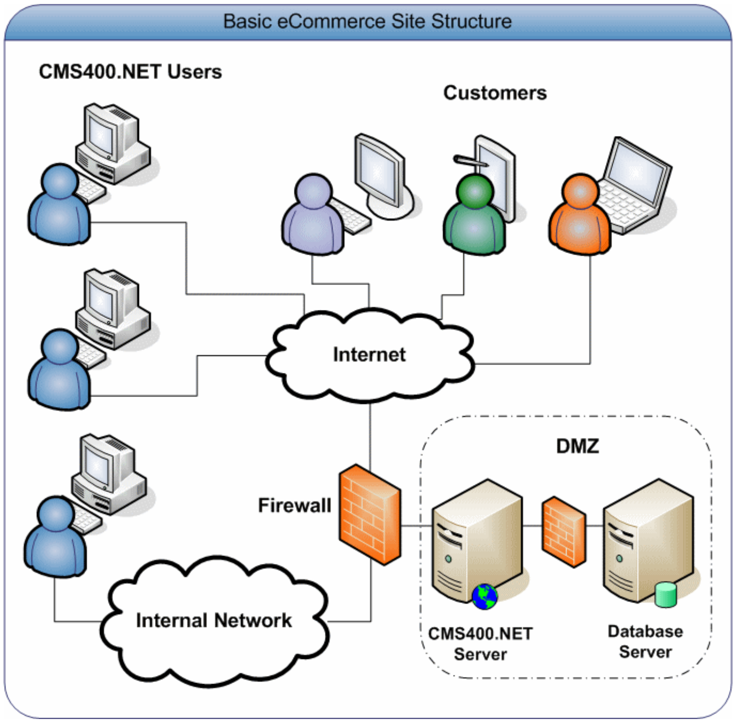
This section contains the following topics:

- Install and Maintain a Firewall Configuration
- Control Direct Access
- Track and Monitor All Network Access
- Wireless Environments
- Using Secure Remote Access
- Encrypt Non-Console Administrative Access
- Encrypt Sensitive Data Sent Over Public Networks
- Remote Updates and Upgrades

- Update Supporting Software with the Latest Patches
- Use HTTP or HTTPS Protocols and Service Ports
- Disable HTTP TRACE/TRACK in Microsoft IIS
- Do Not Allow the Use of the SSL 2.0 Protocol on Your Server
- Never Allow the Use of Live Cardholder Data or Personal Account Numbers for Development, Testing or Troubleshooting

2.1 Install and Maintain a Firewall Configuration

PCI DSS section 1 requires the installation an ongoing maintenance of firewalls to control computer traffic between your internal "trusted" network and external networks. You should also use firewalls to control traffic in and out of the more "sensitive" areas of your internal network. Below is a diagram of a basic eCommerce site structure.



From the PCI DSS Requirement 1:

> *All systems must be protected from unauthorized access from untrusted networks, whether entering the system via the Internet as e-commerce, employees' Internet access through desktop browsers, employees' e-mail access, dedicated connection such as business to business connections, via wireless networks, or via other sources.*

This means that firewalls must be used to segment networks into domains based on each segment's security needs. Firewalls should be placed between the internal network zone and any DMZ and each Internet connection.

2.2 Control Direct Access

PCI DSS section 8.1 and 8.2 requires the assignment of a unique ID and the use of a password or passphrase for anyone accessing system components. Instead of a password or passphrase, you could also use Two-factor authentication, such as, smart cards or biometrics. This helps ensure that each person accessing a system can be identified by their unique account.

The following sections define information about how user accounts and passwords associated with CMS400.NET should be implemented. The term “user” refers to anyone who is a CMS400.NET Administrator or has been added to Commerce Admin role.

- Never Allow the Use of a Group Account
- Passwords Must Be Changed at Least Every Ninety Days
- Passwords Must Be at Least Seven Characters Long
- Use both Numeric and Alphabetic Characters in Passwords
- New Passwords Cannot Match Any of the Last Four Passwords
- Lock Accounts After Six Failed Login Attempts
- Lock Out the Account for at Least Thirty Minutes or Until the Administrator Unlocks It
- After 15 Minutes of an Account Being Idle, Require the User to Re-Enter their Log in Information
- Remove All Default Users

2.2.1 Never Allow the Use of a Group Account

The information in this section relates to PCI DSS section 8.5.8.

A group account is an account that multiple people use to log into CMS400.NET using the same username and password. This is a serious security issue as you lose the ability to accurately keep track of who is doing what in your eCommerce environment.

> As a site owner, you should clearly state in your Web site’s user documentation that use of a group account is forbidden. Ektron clearly states this in the Security Checklist section of the CMS400.NET Setup, Administrator, and User Manuals. The use of a group user account is a violation of Ektron CMS400.NET’s license agreement. **Allowing the use of group user accounts will cause you to be out of compliance with PCI DSS**.

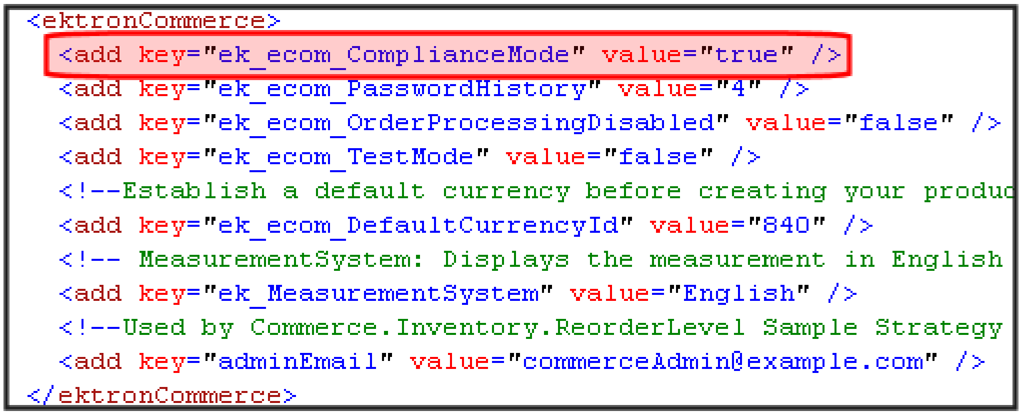
2.2.2 Passwords Must Be Changed at Least Every Ninety Days

The information in this section relates to PCI DSS 8.5.9.

> **Note:** CMS400.NET uses AES encryption to store user’s passwords.

Ektron CMS400.NET has a password security feature that forces an administrator or user with the Commerce Admin role to change their passwords at least every ninety days. This feature is enabled when the `ek_ecom_ComplianceMode` key in the site’s Web.config file is set to true.

The key is highlighted below.



```
<ektronCommerce>
  <add key="ek_ecom_ComplianceMode" value="true" />
  <add key="ek_ecom_PasswordHistory" value="4" />
  <add key="ek_ecom_OrderProcessingDisabled" value="false" />
  <add key="ek_ecom_TestMode" value="false" />
  <!--Establish a default currency before creating your produc
  <add key="ek_ecom_DefaultCurrencyId" value="840" />
  <!-- MeasurementSystem: Displays the measurement in English
  <add key="ek_MeasurementSystem" value="English" />
  <!--Used by Commerce.Inventory.ReorderLevel Sample Strategy
  <add key="adminEmail" value="commerceAdmin@example.com" />
</ektronCommerce>
```

> **Important!** This key must be set to “true” to achieve and maintain PCI DSS certification.

Once an administrator or user with the Commerce Admin role goes eighty-five days without changing their password, a dialog box appears the next time they log in asking them to change their password. If they do not want to change their password at that time, they can click the **Skip** button. They are allowed to do this for the next five days. Once ninety days have passed, they must change their password before they can log into CMS400.NET.

If you are using Active Directory or LDAP to manage users, make sure a password policy is set to force administrators or users with the Commerce Admin role change their password at least every ninety days.

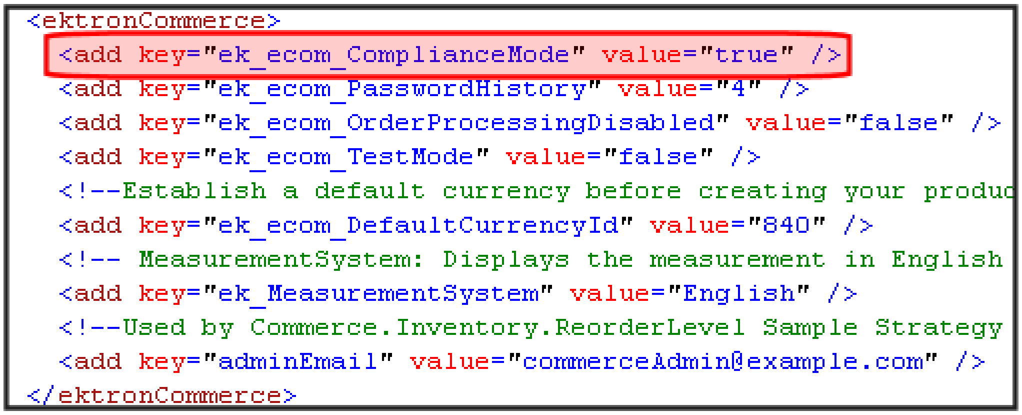
2.2.3 Passwords Must Be at Least Seven Characters Long

The information in this section relates to PCI DSS 8.5.10.

Note: CMS400.NET uses AES encryption to store user's passwords.

Ektron CMS400.NET has a password security feature that forces an administrator or user with the Commerce Admin role to use at least seven characters for their password. This feature is enabled when the `ek_ecom_ComplianceMode` key in the site's Web.config file is set to true.

The key is highlighted below.



```
<ektronCommerce>
  <add key="ek_ecom_ComplianceMode" value="true" />
  <add key="ek_ecom_PasswordHistory" value="4" />
  <add key="ek_ecom_OrderProcessingDisabled" value="false" />
  <add key="ek_ecom_TestMode" value="false" />
  <!--Establish a default currency before creating your produc
  <add key="ek_ecom_DefaultCurrencyId" value="840" />
  <!-- MeasurementSystem: Displays the measurement in English
  <add key="ek_MeasurementSystem" value="English" />
  <!--Used by Commerce.Inventory.ReorderLevel Sample Strategy
  <add key="adminEmail" value="commerceAdmin@example.com" />
</ektronCommerce>
```

Important! This key must be set to "true" to achieve and maintain PCI DSS certification.

If you are using Active Directory or LDAP to manage users, make sure a password policy is set to force administrators or users with the Commerce Admin role to use at least seven characters for their password.

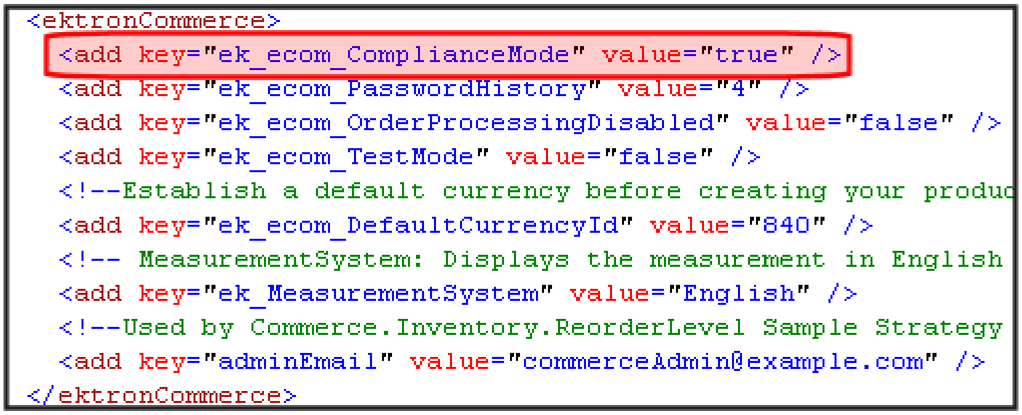
2.2.4 Use both Numeric and Alphabetic Characters in Passwords

The information in this section relates to PCI DSS 8.5.11.

Note: CMS400.NET uses AES encryption to store user's passwords.

Ektron CMS400.NET has a password security feature that forces an administrator or user with the Commerce Admin role to use both numeric and alphabetic characters in their password. This feature is enabled when the `ek_ecom_ComplianceMode` key in the site's Web.config file is set to true.

The key is highlighted below.



```
<ektronCommerce>
  <add key="ek_ecom_ComplianceMode" value="true" />
  <add key="ek_ecom_PasswordHistory" value="4" />
  <add key="ek_ecom_OrderProcessingDisabled" value="false" />
  <add key="ek_ecom_TestMode" value="false" />
  <!--Establish a default currency before creating your produc
  <add key="ek_ecom_DefaultCurrencyId" value="840" />
  <!-- MeasurementSystem: Displays the measurement in English
  <add key="ek_MeasurementSystem" value="English" />
  <!--Used by Commerce.Inventory.ReorderLevel Sample Strategy
  <add key="adminEmail" value="commerceAdmin@example.com" />
</ektronCommerce>
```

Important! This key must be set to “true” to achieve and maintain PCI DSS certification.

If you are using Active Directory or LDAP to manage users, make sure a password policy is set to force administrators or users with the Commerce Admin role to use both numeric and alphabetic characters in their password.

2.2.5 New Passwords Cannot Match Any of the Last Four Passwords

The information in this section relates to PCI DSS 8.5.12.

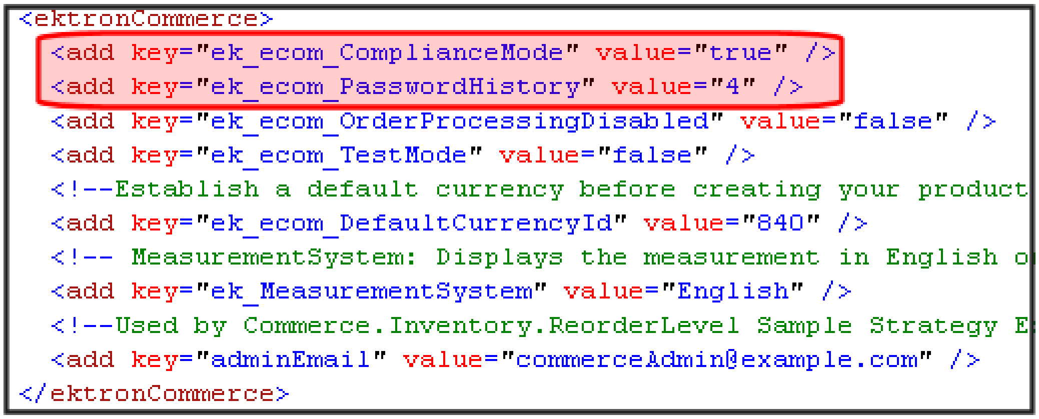
Note: CMS400.NET uses AES encryption to store user’s passwords.

Ektron CMS400.NET has a password security feature that forces an administrator or user with the Commerce Admin role to have a password that does not match any of their last four passwords. This feature is enabled when the site’s Web.config file has the `ek_ecom_ComplianceMode` key set to true and the `ek_ecom_PasswordHistory` key is set to at least four.

You can set the `ek_ecom_PasswordHistory` key to a number higher than four if you want a higher level of security. If you set this key to less than four and the `ek_ecom_ComplianceMode` key is set to true, CMS400.NET will enforce at least four.

If compliance mode is set to…	And password history is set to…	Passwords cannot match the last…
True	4 or higher	4 or higher passwords
True	3 or lower	4 passwords
False	Any number	There will be no effect.

The keys, which are in your Web site’s Web.config file, are highlighted below.



```
<ektronCommerce>
  <add key="ek_ecom_ComplianceMode" value="true" />
  <add key="ek_ecom_PasswordHistory" value="4" />
  <add key="ek_ecom_OrderProcessingDisabled" value="false" />
  <add key="ek_ecom_TestMode" value="false" />
  <!--Establish a default currency before creating your product
  <add key="ek_ecom_DefaultCurrencyId" value="840" />
  <!-- MeasurementSystem: Displays the measurement in English o
  <add key="ek_MeasurementSystem" value="English" />
  <!--Used by Commerce.Inventory.ReorderLevel Sample Strategy E
  <add key="adminEmail" value="commerceAdmin@example.com" />
</ektronCommerce>
```

Important! The `ek_ecom_ComplianceMode` key in the site's Web.config file must be set to "true" to achieve and maintain PCI DSS certification.

If you are using Active Directory or LDAP to manage users, make sure a password policy is set to force administrators or users with the Commerce Admin role to have a password that does not match any of their last four passwords.

2.2.6 Lock Accounts After Six Failed Login Attempts

The information in this section relates to PCI DSS 8.5.13.

Ektron CMS400.NET has a login security feature that, by default, locks out a user after six unsuccessful attempts to log in by a user on one computer.

You control CMS400.NET's login security feature by changing the value of the `ek_loginAttempts` key in the Web.config file. The following table summarizes your options. **To achieve and maintain PCI DSS certification this key must be set to six or less**.

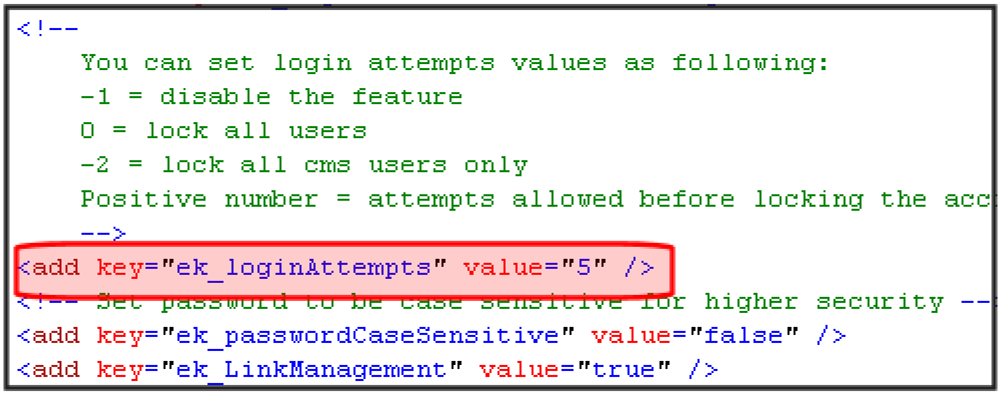
Note: When the `ek_ecom_ComplianceMode` key in the site's Web.config file is set to true and you are using a value greater than six, accounts will be locked after six failed attempts.

The table below contains the values you can use with the `ek_loginAttempts` key.

Value	Description
any number between 1 and 254	The number of times a user can try to log in before he is locked out.
0	Lock out all users. Important! This locks ALL accounts including the Built-in user account.
-1	Disable feature; unlock all locked users.
-2	Lock out CMS users only; membership users can still log in

For example, to allow only three unsuccessful logins, change the value to 3. You cannot enter a value greater than 254.

Note: This feature affects all users who log into CMS400.NET including, Administrators, Content Editors, Membership Users and the Built-in Account. Therefore, it is possible to completely lock yourself out of your site. If this happens, set the `ek_loginAttempts` key in the Web.config file to -1. This unlocks all accounts.



```
<!--
    You can set login attempts values as following:
    -1 = disable the feature
    0 = lock all users
    -2 = lock all cms users only
    Positive number = attempts allowed before locking the acc
    -->
<add key="ek_loginAttempts" value="5" />
<!-- Set password to be case sensitive for higher security --
<add key="ek_passwordCaseSensitive" value="false" />
<add key="ek_LinkManagement" value="true" />
```

If you are using Active Directory or LDAP to manage users, make sure a policy is set that locks out administrators or users with the Commerce Admin role after six unsuccessful attempts to log in to the system.

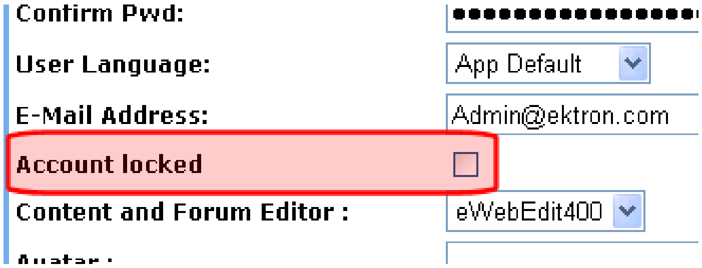
2.2.6.1 Locking an Individual's Account in Ektron CMS400.NET

There are three ways a user account can become locked:

- A user fails to properly login in after a specified number of attempts
- The Web.config file's `ek_loginAttempts` key is set to 0 (zero)
- An administrator manually locks the account

To manually lock a user's account:

1. Log in to the CMS400.NET Workarea as an Administrator.
2. If the individual is a CMS400.NET user or Administrator, navigate to **Settings** > **Users**.
   If the individual is a Membership user (registered site visitor, customer), navigate to **Modules** > **Community Management** > **Memberships** > **Users**.
3. Click the individual's Username.
4. Click the **Edit** button (📝).
5. Click the **Account Locked** check box. If a check is in the box, the account will be locked upon saving.



Confirm Pwd:	●●●●●●●●●●●●●●●●
User Language:	App Default
E-Mail Address:	Admin@ektron.com
Account locked	□
Content and Forum Editor :	eWebEdit400
Avatar :	

6. Click the **Save** button (💾).

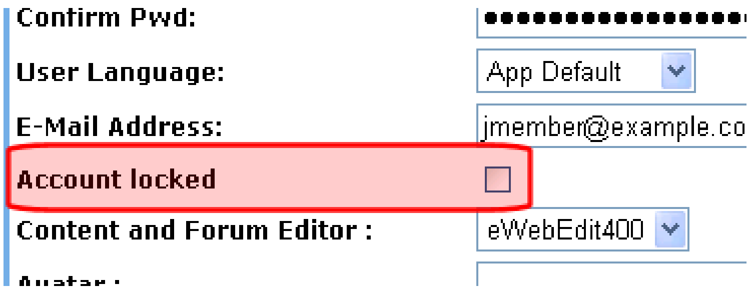
2.2.6.2 Unlocking an Individual's Account in Ektron CMS400.NET

There are two ways to unlock an individual's account:

- Setting the Web.config file's `ek_loginAttempts` key to -1. Note that this unlocks all locked users.
- Manually unlocking an individuals account.

To manually unlock a user's account:

1. Log into the CMS400.NET Workarea as an Administrator.
2. If the individual is a CMS400.NET user or Administrator, navigate to **Settings** > **Users**.
   If the individual is a Membership user (registered site visitor, customer), navigate to **Modules** > **Community Management** > **Memberships** > **Users**.
3. Click the individual's Username.
4. Click the **Edit** button (📝).
5. Click the **Account Locked** check box to remove the checkmark. If the box is empty, the account will be unlocked upon saving.



Confirm Pwd: ●●●●●●●●●●●●●●●●

User Language: App Default

E-Mail Address: jmember@example.co

Account locked □

Content and Forum Editor : eWebEdit400

Avatar :

6.Click the **Save** button (💾).

2.2.7 Lock Out the Account for at Least Thirty Minutes or Until the Administrator Unlocks It

The information in this section relates to PCI DSS 8.5.14.

Once an account is locked in Ektron CMS400.NET, an administrator must manually unlock it. There are no settings to allow for automatically unlocking account. To learn how to unlock an account, see Unlocking an Individual's Account in Ektron CMS400.NET.

2.2.8 After 15 Minutes of an Account Being Idle, Require the User to Re-Enter their Login Information

The information in this section relates to PCI DSS 8.5.15.

Ektron CMS400.NET has a password security feature that automatically logs an administrator or user with the Commerce Admin role out of the application after 15 minutes of inactivity. Inactivity is based on requests that are made to the server.

> **Important!** The `ek_ecom_ComplianceMode` key in the site's Web.config file must be set to "true" to achieve and maintain PCI DSS certification.

This feature is enabled in Ektron CMS400.NET when the site's Web.config file has the `ek_ecom_ComplianceMode` key is set to true. In addition:

- If you are using IIS 7, the line in green below needs to appear between the `<modules>` tags in the Web.config file. This line is a part of the default install; you should make sure it has not been removed. **If you are using IIS 7 and remove this line, you will not achieve and maintain PCI DSS certification.**

```
<modules>
<add name="MyDigestAuthenticationModule"
type="Ektron.ASM.EkHttpDavHandler.Security.DigestAuthenticationModule,Ektron.ASM.EkHttpDavHandler"
/>

<add name="ScriptModule" type="System.Web.Handlers.ScriptModule, System.Web.Extensions,
Version=1.0.61025.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35"
preCondition="integratedMode" />

<add name="EkUrlAliasModule" type="UrlAliasingModule" preCondition="integratedMode" />
</modules>
```

- If you are using IIS 6, the line in green below needs to appear between the `<httpModules>` tags in the Web.config file. This line is a part of the default install; you should make sure it has not been

```
<httpModules>
<add name="DigestAuthenticationModule"
type="Ektron.ASM.EkHttpDavHandler.Security.DigestAuthenticationModule,Ektron.ASM.EkHttpDavHandler
" />

<add name="ScriptModule" type="System.Web.Handlers.ScriptModule, System.Web.Extensions,
Version=1.0.61025.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35"/>

<add name="EkUrlAliasModule" type="UrlAliasingModule" />
</httpModules>
```

2.2.9 Remove All Default Users

All default users supplied with any software that will reside on a server hosting CMS400.NET should be removed. If they cannot be removed, they should be disabled, or at least renamed and given new passwords. To learn how to change or remove default users supplied with Ektron CMS400.NET, see the following topics in this book.

- Change the Builtin User Account Information
- Change the Administrator’s Username and Password
- Remove the Demonstration User - jedit
- Remove the Demonstration Membership User - jmember

2.3 Track and Monitor All Network Access

PCI DSS section 10 requires the tracking of a user’s activities on your network. This is vital to keeping your site secure and will help you determine the source when data is compromised. While it is important that this information is captured, **it is even more important that you review it, analyze it and use it.** For example, while reviewing eCommerce event logs in CMS400.NET, you might find that one of your eCommerce administrators has an unusually large amount of login failures. This could be a sign someone is using his username to try to break into your system.

Make sure you implement automated audit trails on all system configurations for the following events:

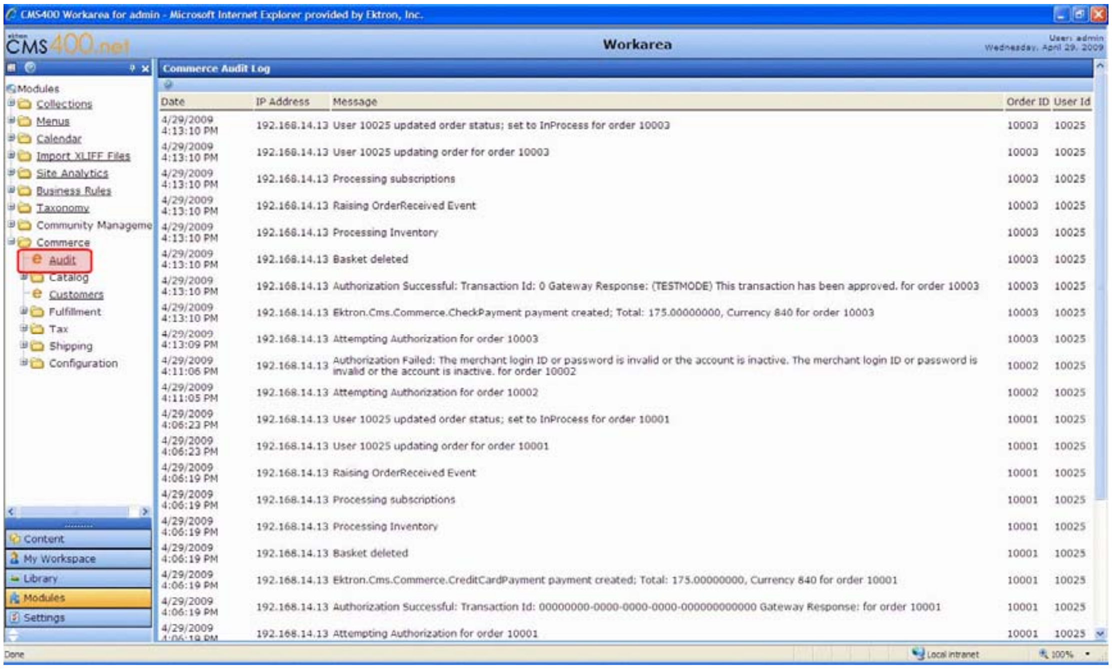
- All actions taken by individuals with administrative privileges
- Accessing audit trails
- Invalid logical access attempts
- Use of identification and authentication mechanisms
- Initialization of the audit logs
- Creation and deletion of system-level objects

Make sure at least following information is captured for each log entry:

- User identification
- Type of event
- Date and time
- Success or failure indication
- Origination of event
- Identity or name of affected data, system component, or resource

2.3.1 Viewing Your Ektron CMS400.NET Web Site’s eCommerce Activity Logs

You can view a log of your CMS400.NET Web site’s eCommerce activity in the **Workarea** > **Modules** > **Commerce** > **Audit** screen.



Commerce Audit Log

Date	IP Address	Message	Order ID	User Id
4/29/2009 4:13:10 PM	192.168.14.13	User 10025 updated order status; set to InProcess for order 10003	10003	10025
4/29/2009 4:13:10 PM	192.168.14.13	User 10025 updating order for order 10003	10003	10025
4/29/2009 4:13:10 PM	192.168.14.13	Processing subscriptions	10003	10025
4/29/2009 4:13:10 PM	192.168.14.13	Raising OrderReceived Event	10003	10025
4/29/2009 4:13:10 PM	192.168.14.13	Processing Inventory	10003	10025
4/29/2009 4:13:10 PM	192.168.14.13	Basket deleted	10003	10025
4/29/2009 4:13:10 PM	192.168.14.13	Authorization Successful: Transaction Id: 0 Gateway Response: (TESTMODE) This transaction has been approved. for order 10003	10003	10025
4/29/2009 4:13:10 PM	192.168.14.13	Ektron.Cms.Commerce.CheckPayment payment created; Total: 175.00000000, Currency 840 for order 10003	10003	10025
4/29/2009 4:13:09 PM	192.168.14.13	Attempting Authorization for order 10003	10003	10025
4/29/2009 4:11:06 PM	192.168.14.13	Authorization Failed: The merchant login ID or password is invalid or the account is inactive. The merchant login ID or password is invalid or the account is inactive. for order 10002	10002	10025
4/29/2009 4:11:05 PM	192.168.14.13	Attempting Authorization for order 10002	10002	10025
4/29/2009 4:06:23 PM	192.168.14.13	User 10025 updated order status; set to InProcess for order 10001	10001	10025
4/29/2009 4:06:23 PM	192.168.14.13	User 10025 updating order for order 10001	10001	10025
4/29/2009 4:06:19 PM	192.168.14.13	Raising OrderReceived Event	10001	10025
4/29/2009 4:06:19 PM	192.168.14.13	Processing subscriptions	10001	10025
4/29/2009 4:06:19 PM	192.168.14.13	Processing Inventory	10001	10025
4/29/2009 4:06:19 PM	192.168.14.13	Basket deleted	10001	10025
4/29/2009 4:06:19 PM	192.168.14.13	Ektron.Cms.Commerce.CreditCardPayment payment created; Total: 175.00000000, Currency 840 for order 10001	10001	10025
4/29/2009 4:06:19 PM	192.168.14.13	Authorization Successful: Transaction Id: 00000000-0000-0000-0000-000000000000 Gateway Response: for order 10001	10001	10025
4/29/2009 4:06:19 PM	192.168.14.13	Attempting Authorization for order 10001	10001	10025

For eCommerce activity logging to be activated for your site, your Web.config file’s `ek_ecom_ComplianceMode` key must be set to “true”.

Important! The `ek_ecom_ComplianceMode` key in the site’s Web.config file must be set to “true” to achieve and maintain PCI DSS certification.

When compliance mode is turned on, Ektron CMS400.NET logs the following events:

- Actions affecting Administrators (Administrator Group member, Commerce Admin Role, Builtin Account)
  - An Administrator logs in or out
  - An Administrator’s login attempt fails
  - An Administrator password is changed
- Actions affecting User rights to eCommerce
  - Adding a user to the Commerce Admin Role
  - Removing a user from the Commerce Admin Role
  - Adding a user to the Admin group
  - Removing a user from the Admin group
- Actions affecting order information
  - Updates to an order’s address
  - The transaction ID and response from the payment gateway
  - Any action conducted with the payment gateway; for example, when capturing a transaction that has been previously authorized
  - Workflow activities; for example, sending out an email
  - Whenever the default gateway or payment options are changed in the Workarea

2.4 Wireless Environments

Ektron CMS400.NET has no wireless configurations as shipped. Do not use CMS400.NET in a wireless environment for eCommerce purposes. If you use CMS400.NET in a wireless environment, Ektron's PA DSS certification will not apply.

From the PCI DSS:

> *"Before wireless technology is implemented, a company should carefully evaluate the need for the technology against the risk. Consider deploying wireless technology only for non-sensitive data transmission."*

PCI DSS section 1.3.8 requires that cardholder data be encrypted when transmitted over wireless connections. Wireless devices must have strong encryption enabled in their security settings for authentication and transmission. Below is a list of requirements for maintaining PCI DSS compliance in a wireless environment:

- Do not use default encryption keys.
- Encryption keys should be changed anytime someone who knows the keys leaves the company.
- Change SNMP community strings on wireless devices.
- Default settings and passwords must be changed on wireless devices.
- The wireless devices firmware supports strong encryption for authentication and transmission. (e.g. WPA/WPA2)
- Make sure you use industry standard best practices, such as IEEE 802.11i, when transmitting cardholder data over wireless networks.
- For new wireless installations, do not use WEP after March 31st 2009
- For existing wireless installation, do not use WEP after June 30th 2010

2.5 Using Secure Remote Access

CMS400.NET Administrators and users should only remotely access the system through the Workarea client via a secure browser. This is the only remote access Ektron provides to CMS400.NET on a server. When an administrator or user with the Commerce Admin Role accesses the Workarea from a remote system, their actions are logged. For a list of items that are logged, see Viewing Your Ektron CMS400.NET Web Site's Activity Logs

If you use another company's remote console software to create a connection to a server containing CMS400.NET, you should follow the PCI DSS requirements for using remote access securely.

Allow connections only from specific known IP and/or MAC addresses. Ektron CMS400.NET does not allow you to block or allow specific IP or MAC addresses. This can easily be accomplished through the use of firewalls and routers. If you do not limit your Web site's administrative access to only known IP or MAC addresses, your Web site will not be PCI DSS compliant. This includes CMS400.NET Administrators and users with the Commerce Administrator Role.

When allowing a vendor remote access for the purpose of troubleshooting software or hardware issues, require two-factor authentication and make sure the remote account is only active while the specific access is required. Also, only grant the access needed to fix the issue.

Important! When using a remote connection to troubleshoot, never use actual live card holder data. Typically, your credit card processor can provide you with test card holder data for troubleshooting.

Below are some remote access security features.

- Incorporate two-factor authentication. For example, you might use a username and password combined with an additional item, such as smart card, certificate or token.
- Do not use the remote access software's default passwords.
- Make the passwords unique to that application. That way, if someone learns the password they cannot use it to gain entry into other systems.
- Use strong passwords according to PCI DSS Requirements 8.1, 8.3, and 8.5.8–8.5.15
    - CMS400.NET does this for automatically for Administrators and Users with the Commerce Administrator Role. *See Also*:
        - Passwords Must Be Changed at Least Every Ninety Days
        - Passwords Must Be at Least Seven Characters Long
        - Use both Numeric and Alphabetic Characters in Passwords
        - New Passwords Cannot Match Any of the Last Four Passwords
- Turn on data transmission encryption as explained in section 4.1 of the PCI DSS.
- Enable account lockout after a certain number of failed login attempts according to PCI DSS Requirement 8.5.13
- Require VPN connections via a firewall.
- Make sure logging is enabled so you can review actions performed remotely.
- Revoke access once the remote task is complete.

2.6 Encrypt Non-Console Administrative Access

PCI DSS section 2.3 requires that you must encrypt all non-console administrative access by using any of the following technologies:

- Secure Shell
- Virtual Private Network
- Secure Socket Layer
- Transport Layer Security

Ektron CMS400.NET uses SSL for encryption. For information on using SSL with CMS400.NET, see Use 128 bit SSL Encryption.

Never allow the use of Telnet or rlogin for non-console administration.

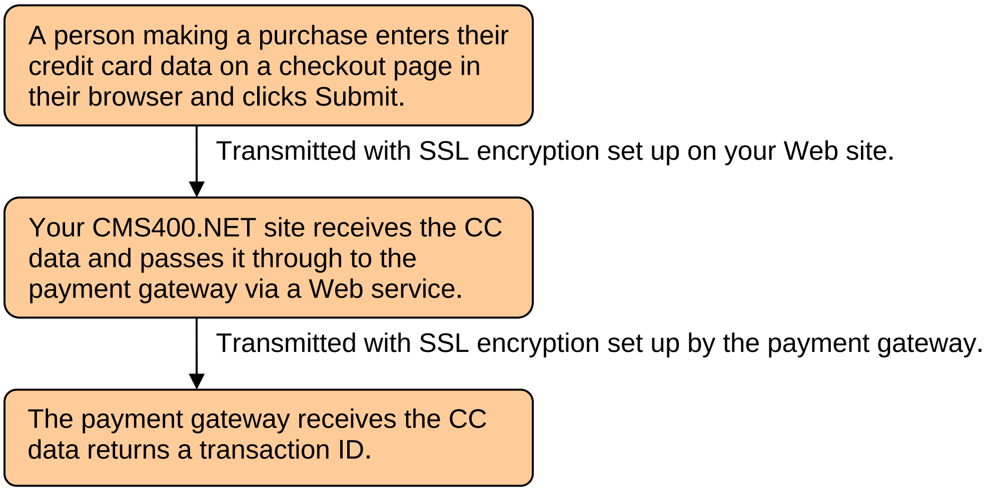
2.7 Encrypt Sensitive Data Sent Over Public Networks

PCI DSS 4.1 requires that you use of strong cryptography and security protocols when transmitting cardholder data over a public network. For example, you could use SSL/TLS or IPSEC to safeguard this data during transmission. Some examples of public networks include:

- The Internet
- Various Wireless technologies
- Global System for Mobile Communications (GSM)
- General Packet Radio Service (GPRS)

When using the eCommerce feature in CMS400.NET, use 128 bit SSL Encryption. This provides a secure mode of transmission for card holder data from a customer's Web browser to your server. For information on using SSL with CMS400.NET, see Use 128 bit SSL Encryption.

Below is flow chart showing where the SSL encryption you install on your Web site is used during the purchase process.



A person making a purchase enters their credit card data on a checkout page in their browser and clicks Submit.

Transmitted with SSL encryption set up on your Web site.

Your CMS400.NET site receives the CC data and passes it through to the payment gateway via a Web service.

Transmitted with SSL encryption set up by the payment gateway.

The payment gateway receives the CC data returns a transaction ID.

In addition, always use strong encryption for sensitive card data sent via end-user messaging technologies. **Ektron CMS400.NET does not send cardholder data through email or any other messaging service.**

2.8 Remote Updates and Upgrades

Because CMS400.NET does not allow for remote updates or upgrades through its Workarea, you will need to download updates or upgrades and install them on the machine hosting your CMS400.NET Web site. When downloading updates or upgrades, insure the machine connecting to Ektron's Web site is behind a firewall. A server used for running CMS400.NET should never connect directly to the internet. It should reside behind a firewall.

2.9 Update Supporting Software with the Latest Patches

Update all supporting software with the latest updates and patches on a bi-weekly basis. Supporting software consists of any software that's used to run or interact with CMS400.NET. Some examples are:

- Operating System
    - For example, Microsoft Windows Server 2008
- Database Software
    - For example, Microsoft SQL Server 2005
- Web Server Software
    - For example, Microsoft IIS
- Web Browsers Software
    - For example, Microsoft Internet Explorer
- Web Application Software
    - For example, Microsoft ASP .NET Framework
- Active Directory or LDAP Software
- Web Site Development Tools
    - For example, Microsoft Visual Studio

If all supporting software consists of Microsoft products, you can schedule the Windows Update and Microsoft Update tools to run on a bi-weekly basis. You should also train your users who connect directly to CMS400.NET to update their browsers with the latest security patches.

2.10 Use HTTP or HTTPS Protocols and Service Ports

Ektron CMS400.NET is designed to use the HTTP or HTTPS protocols and its associated ports. You should disable access to any other protocols and ports that are not absolutely necessary to running your Web site. By disabling unused protocols and ports, you closing potential vulnerabilities related to your site.

2.11 Disable HTTP TRACE/TRACK in Microsoft IIS

The TRACE method (verb) allows debugging and connection trace analysis for connections from a client to a Web server. This method is part of the HTTP specification and causes a Web server to relay information sent to it by a client system. Microsoft uses the TRACK method (verb) as an alias for TRACE in IIS. These methods are identical. One of the security issues related to TRACE/TRACK is that the method can be used by a corrupted component in a Web page to relay authentication information to a third party when an unsuspecting user logs in.

To disable HTTP TRACE/TRACK in IIS 6.0, you will need to install the Microsoft UrlScan Filter and follow the steps below.
Important: You should review the documentation associated with this software. Microsoft Urlscan Filter is a security tool that **restricts the types of HTTP requests that Internet Information Services (IIS) will process**. By blocking specific HTTP requests, UrlScan helps prevent potentially harmful requests from being processed by web applications on the server.

1. Download and install the Microsoft UrlScan Filter. http://www.microsoft.com/downloads/details.aspx?FamilyId=EE41818F-3363-4E24-9940-321603531989&displaylang=en
2. Once the install is complete, open the UrlScan.ini file located in <Windows Server install drive>:\Windows\system32\inetsrv\urlscan.
3. Set the `UseAllowVerbs` parameter to **0** (zero). This causes UrlScan to use the [DenyVerbs] list instead of [AllowVerbs].
4. Scroll down to the **[DenyVerbs]** section.
5. In that section, add the **TRACE** and **TRACK** methods.
6. Save and close the file.
7. Restart Internet Information Service (IIS)

To disable HTTP TRACE/TRACK in IIS 7.0 follow these steps.
Note: These instructions are from Microsoft's www.iis.net Web site and are Copyright 2009 Microsoft Corporation.

1. On the Taskbar, click **Start** > **Administrative Tools** > **Internet Information Services (IIS) Manager**.
2. In the Connections pane, go to the connection, site, application, or directory for which you want to modify your request filtering settings.
3. In the Home pane, double-click Request Filtering.
4. In the Request Filtering pane, click the **HTTP Verbs** tab.
5. Click **Deny Verb...** in the Actions pane.
6. In the Deny Verb dialog box, enter **TRACE**.
7. Click **OK**.
8. Click **Deny Verb...** in the Actions pane.
9. In the Deny Verb dialog box, enter **TRACK**.
10. Click **OK**.

2.12 Do Not Allow the Use of the SSL 2.0 Protocol on the Server

Microsoft Windows Servers allow the use of SSL 2.0 by default. To be PCI DSS compliant, you must disable it on any servers you're using to run CMS400.NET. Information about the SSL 2.0 protocol is stored in the registry key:

```
HKey_Local_Machine\System\CurrentControlSet\Control\SecurityProviders \SCHANNEL\Protocols\SSL 2.0
```

To disable SSL 2.0, follow the steps below.

1. On the Taskbar, click **Start** > **Run**.
2. Type **regedit**.
3. Click **OK**.
4. In the Registry Editor, navigate to the following key.

   ```
   HKey_Local_Machine\System\CurrentControlSet\Control\SecurityProviders
   \SCHANNEL\Protocols\SSL 2.0\Server
   ```

5. Inside the Server folder window, right click and select **New** > **DWORD Value**.
6. Change the name of the value to **Enabled**.
7. Make sure the Data column shows **0x00000000 (0)**. If it does not, right click the value and select **Modify**. Then, enter **0** (zero) as the Value data.
8. Restart the server.

2.13 Never Allow the Use of Live Cardholder Data or Personal Account Numbers for Development, Testing or Troubleshooting

While developing, testing or troubleshooting your Web site, **never** allow the use of live cardholder data or personal account numbers. Typically, your credit card processor can provide you with test cardholder data for development, testing and troubleshooting. It is important to educate your developers, quality assurance personnel, and support people about not using live cardholder data or personal account numbers.

3 Setting Up and Configuring Ektron CMS400.NET

This section explains how to set up and configure Ektron CMS400.NET so it can be used in a PCI DSS compliant environment.

- Make Sure Your Hosting Server is PCI Compliant
- Install Ektron CMS400.NET
- Use 128 bit SSL Encryption
- Steps to Set up a Basic eCommerce Web Site
- Test Your Payment Gateway
- Administrators vs. the Commerce Admin Role
- Understanding Ektron CMS400.NET in an eCommerce Environment
- Train Your Personnel

3.1 Make Sure Your Hosting Server is PCI Compliant

If you are hosting Ektron CMS400.NET on your own server, make sure the server environment is PCI DSS Compliant. If your site will be hosted, select a hosting provider that offers a PCI DSS Compliant environment.

3.2 Install Ektron CMS400.NET

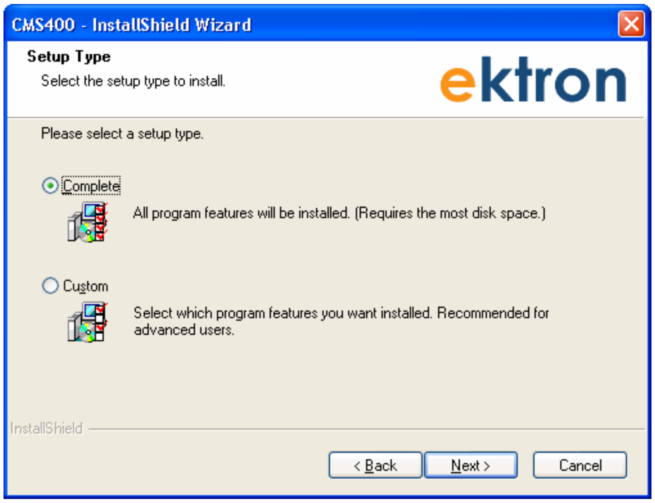
Here are the basic steps needed to setup a Web site with CMS400.NET v7.6.5 or later. These steps explain how to set up Ektron's "Min" site. The "Min" site is designed to be a blank starting point for creating a Web site. Additional setup details can be found in the Ektron CMS400.NET Setup Manual. Ektron CMS400.NET needs to be installed to a Full Trust ASP.NET host.

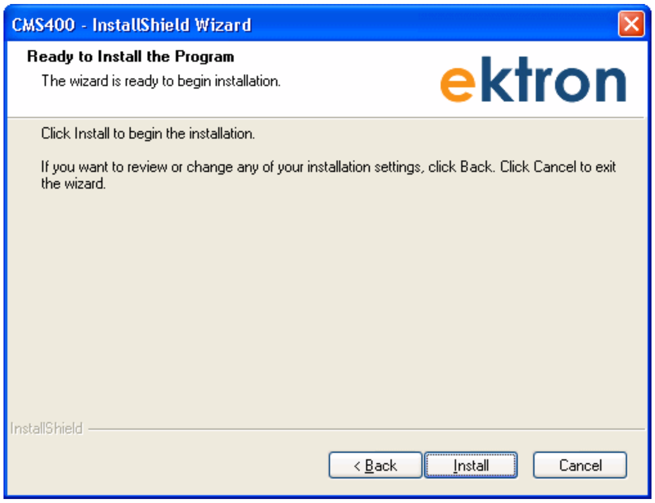
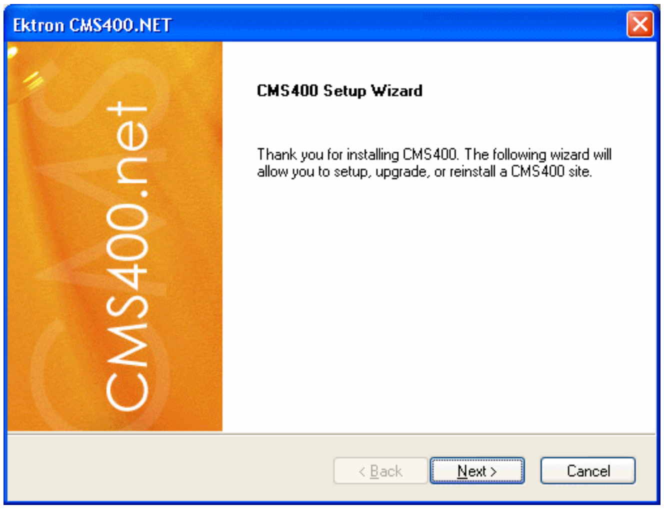
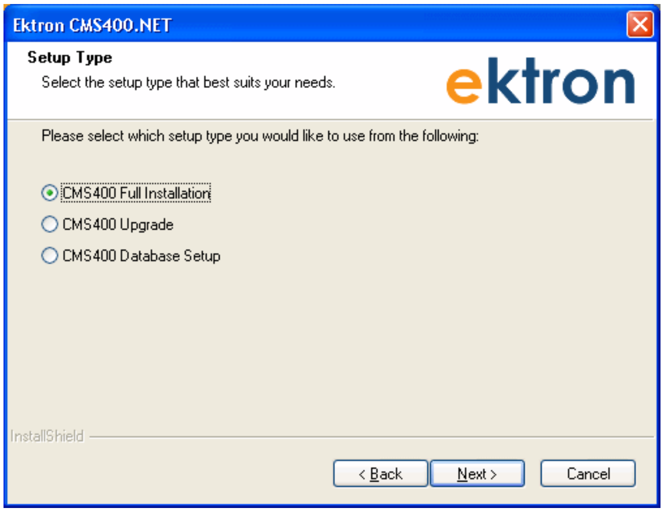
This section includes:

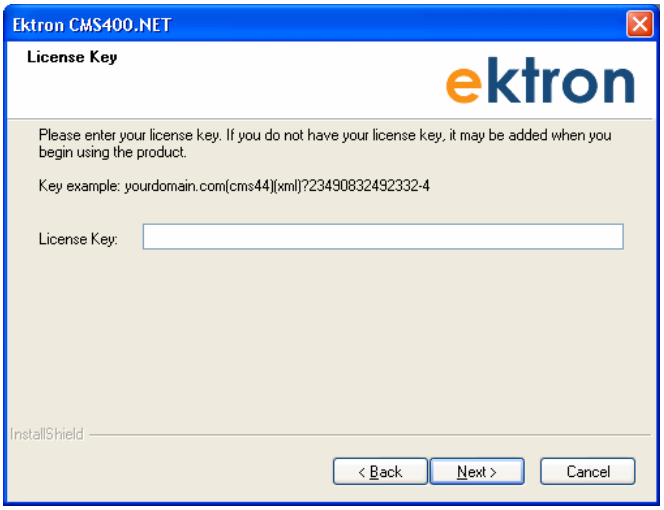
- Steps to Install the CMS400.NET Min Site
- Once the Install is Complete

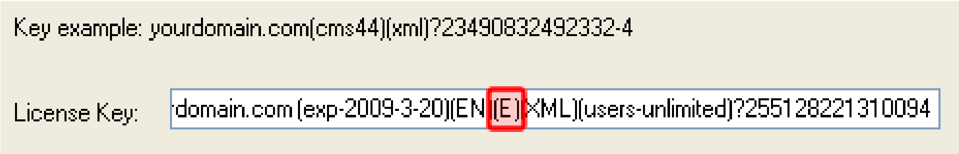
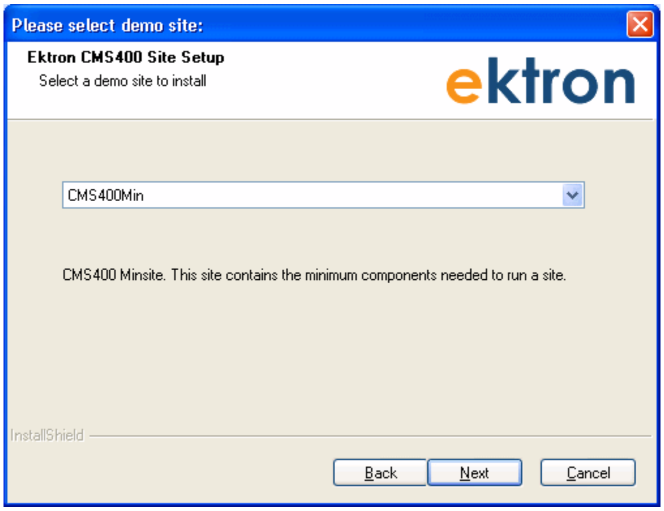
3.2.1 Steps to Install the CMS400.NET Min Site

These steps assume you have downloaded the CMS400Basev76.exe.

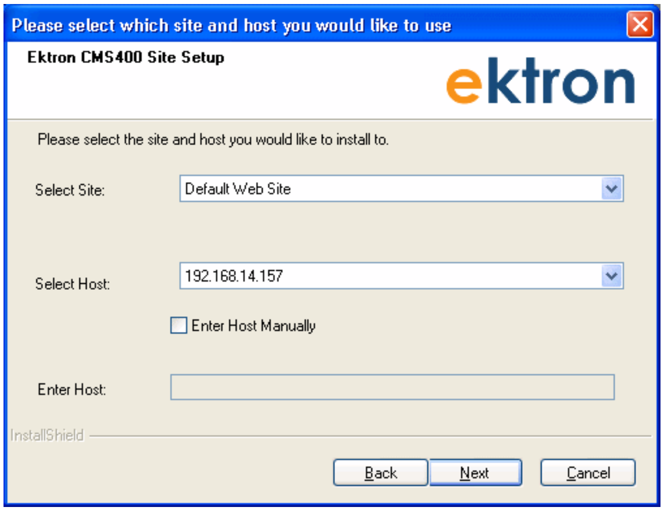
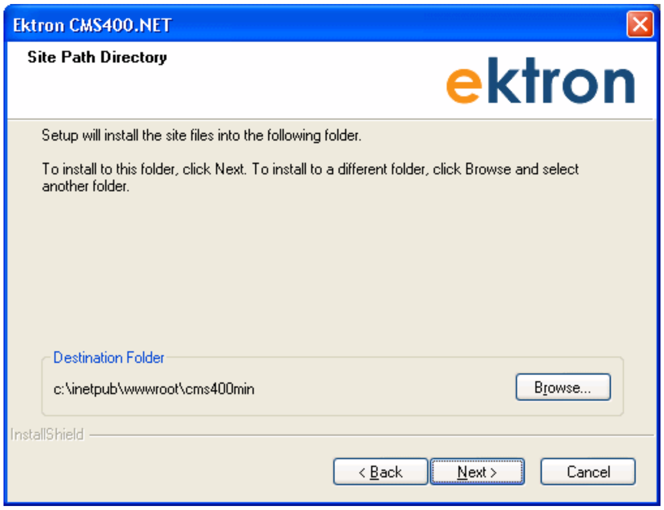
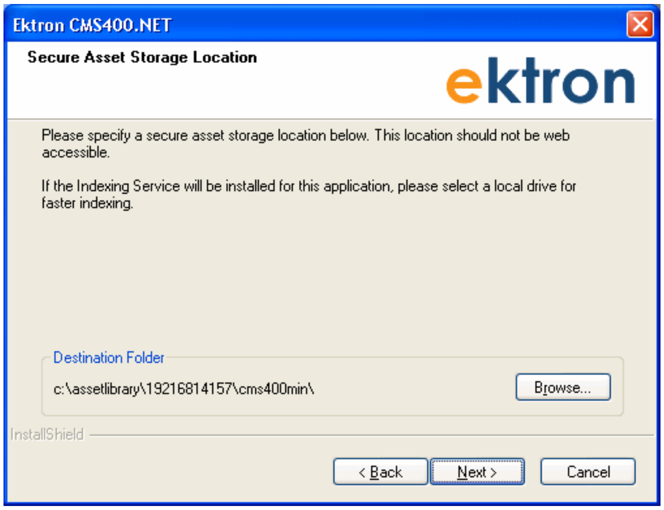
Steps	Setup Screen
1. Double click the CMS400Basev76.exe file to start the installation.	
2. Click the "I accept the terms of the license agreement" radio button and click **Next.**	
3. In the "Setup Type" screen, select "Complete" and click **Next.**	 CMS400 - InstallShield Wizard Setup Type Select the setup type to install. Please select a setup type. ● Complete All program features will be installed. (Requires the most disk space.) ○ Custom Select which program features you want installed. Recommended for advanced users.

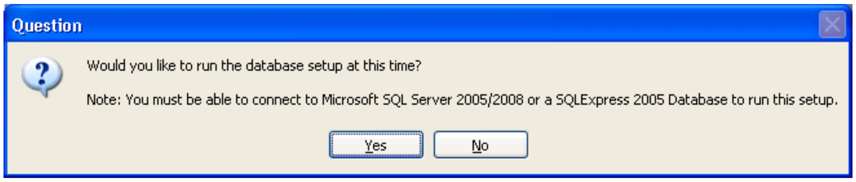
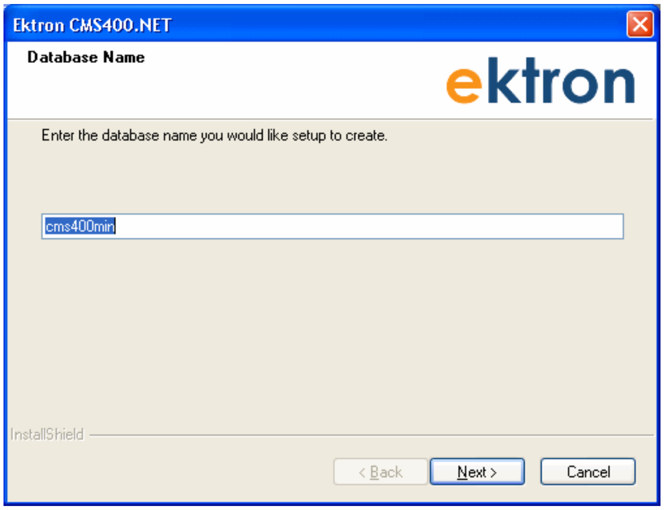
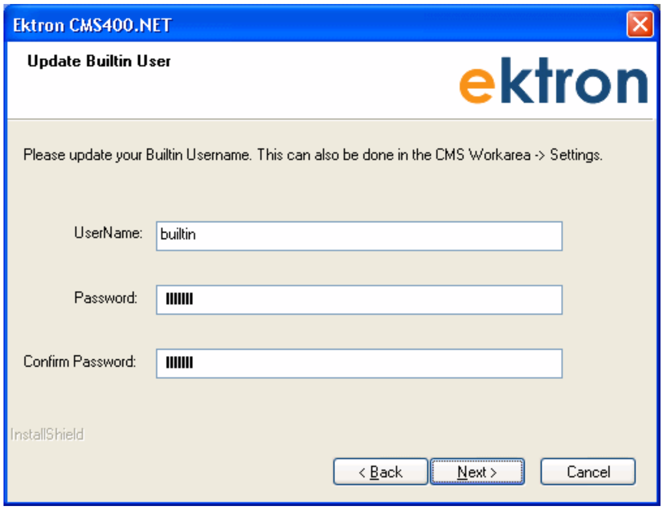
<table>
<tr><td>4. In the “Ready to Install the Program” screen, click <b>Install</b>.</td><td>
CMS400 - InstallShield Wizard
<b>Ready to Install the Program</b>
The wizard is ready to begin installation.
Click Install to begin the installation.
If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.
 </td></tr>
<tr><td colspan="2">5. Click <b>Yes</b> to have the install check for updates.</td></tr>
<tr><td colspan="2">6. If your system needs to shutdown and restart, do so. Your system will automatically continue with the Site Setup portion of the install.</td></tr>
<tr><td>7. Click the <b>Next</b> button in the “CMS400 Setup Wizard” screen.</td><td>
Ektron CMS400.NET
<b>CMS400 Setup Wizard</b>
Thank you for installing CMS400. The following wizard will allow you to setup, upgrade, or reinstall a CMS400 site.
 </td></tr>
<tr><td>8. Select the <b>CMS400 Full Installation</b> radio button from the “Setup Type” screen and click <b>Next</b>.</td><td>
Ektron CMS400.NET
<b>Setup Type</b>
Select the setup type that best suits your needs.
Please select which setup type you would like to use from the following:
● CMS400 Full Installation
○ CMS400 Upgrade
○ CMS400 Database Setup
 </td></tr>
</table>

<table>
<tr>
<td>9. In the “License Key” screen, enter your license key in the text box and click <b>Next</b>.</td>
<td>


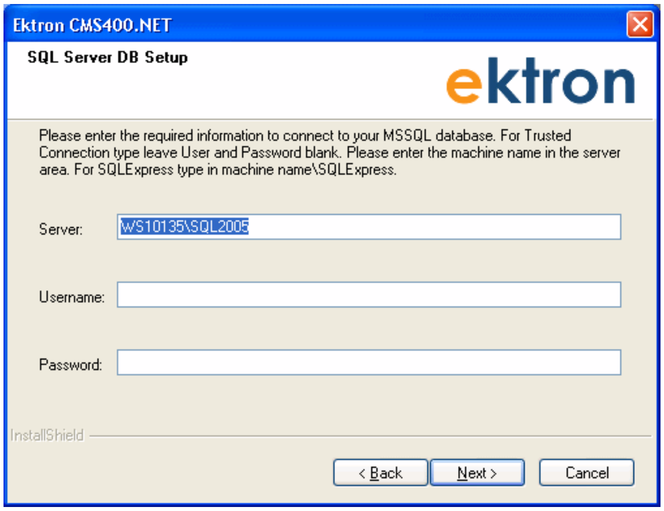
Please enter your license key. If you do not have your license key, it may be added when you begin using the product.
Key example: yourdomain.com(cms44)(xml)?23490832492332-4
License Key:
</td>
</tr>
<tr>
<td colspan="2"><b>Important!</b> Make sure you enter a license key that contains the (E) modifier into the License Key window. This enables the eCommerce functionality for your Web site.

Key example: yourdomain.com(cms44)(xml)?23490832492332-4
License Key: domain.com(exp-2009-3-20)(EN)(E)(XML)(users-unlimited)?255128221310094
</td>
</tr>
<tr>
<td>10. Select <b>CMS400Min</b> from the Select a Demo Site screen and click <b>Next</b>.</td>
<td>


CMS400Min
CMS400 Minsite. This site contains the minimum components needed to run a site.
</td>
</tr>
</table>

11. In the “Select Site and Host” screen, use the defaults and click **Next**.	 Please select which site and host you would like to use Ektron CMS400 Site Setup Please select the site and host you would like to install to. Select Site: Default Web Site Select Host: 192.168.14.157 □ Enter Host Manually Enter Host:
12. In the “Site Path Directory” screen, use the default and click **Next**.	 Ektron CMS400.NET Site Path Directory Setup will install the site files into the following folder. To install to this folder, click Next. To install to a different folder, click Browse and select another folder. Destination Folder c:\inetpub\wwwroot\cms400min ektron Browse... InstallShield < Back Next > Cancel
13. In the “Secure Asset Storage Location” screen, use the default and click **Next**.	 Ektron CMS400.NET Secure Asset Storage Location Please specify a secure asset storage location below. This location should not be web accessible. If the Indexing Service will be installed for this application, please select a local drive for faster indexing. Destination Folder c:\assetlibrary\19216814157\cms400min\ ektron Browse... InstallShield < Back Next > Cancel

14. A dialog appears asking if you want to run the database setup, click **Yes**.	 Would you like to run the database setup at this time? Note: You must be able to connect to Microsoft SQL Server 2005/2008 or a SQLExpress 2005 Database to run this setup.
15. In the "Database Name" screen, enter the name of the database and click **Next**. For this example, we are using cms400min. In a real world installation, make sure you change the name of the database Do not use the default. For example, do not use cms400min.	 Ektron CMS400.NET Database Name ektron Enter the database name you would like setup to create. cms400min InstallShield < Back Next > Cancel
16. In the "Update Builtin User" information screen change the Name and Password, and then click **Next**.	 Ektron CMS400.NET Update Builtin User ektron Please update your Builtin Username. This can also be done in the CMS Workarea -> Settings. UserName: builtin Password: ||||||| Confirm Password: ||||||| InstallShield < Back Next > Cancel

17. In the “SQL Server DB Setup” screen, enter the required Server, Username and Password information needed to connect to your database and click **Next**.



Ektron CMS400.NET

SQL Server DB Setup

Please enter the required information to connect to your MSSQL database. For Trusted Connection type leave User and Password blank. Please enter the machine name in the server area. For SQLExpress type in machine name\SQLExpress.

Server: WS10135\SQL2005

Username:

Password:

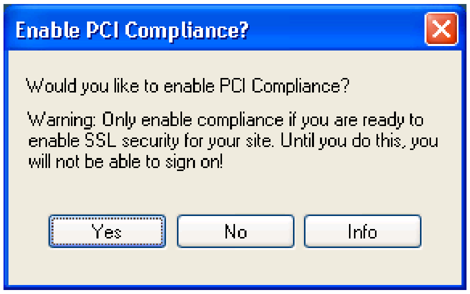
18. A dialog appears asking if you want to install the CMS400.NET SDK. If you do, proceed with that install, then return to step 19. That install is not covered for the purposes of this document.

19. A dialog appears asking if you want to enable PCI compliance.

Important: Enabling compliance requires you to have an SSL certificate installed for your web site.

Note: Selecting Yes changes the following Web.config key to “true”

```
<add key=“ek_ecom_ComplianceMode” value=“false” />
<add key=“UseSSL” value=“false” />
```

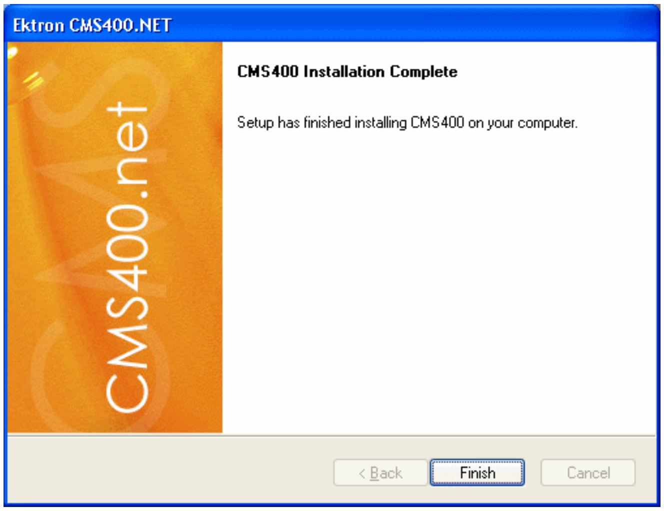


Enable PCI Compliance?

Would you like to enable PCI Compliance?

Warning: Only enable compliance if you are ready to enable SSL security for your site. Until you do this, you will not be able to sign on!

20. Once the CMS400 Installation Complete screen appears, click **Finish**. This is the end of the installation for the purposes of this document.



Ektron CMS400.NET

CMS400 Installation Complete

Setup has finished installing CMS400 on your computer.

Note: A dialog appears asking if you want to run the eSync certificate tool. If you are using eSync, proceed; otherwise, click No. This information is covered in the CMS400.NET eSync Manual.

3.2.2 Once the Install is Complete

Below is a list of items that should be done once the install is complete.

- Change the Builtin User Account Information
- Change the Administrator’s Username and Password
- Remove the Demonstration User - jedit
- Remove the Demonstration Membership User - jmember

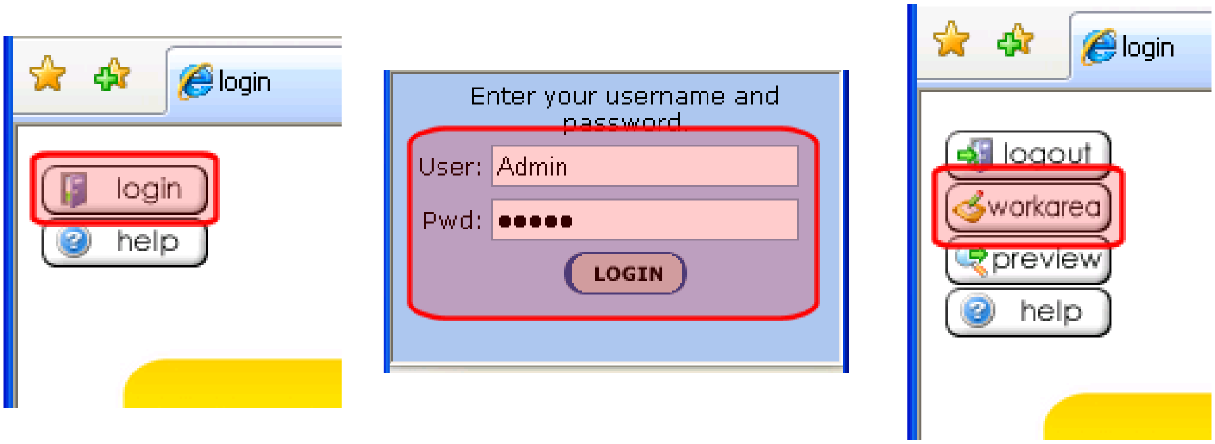
3.2.2.1 Change the Builtin User Account Information

If you did not change the Builtin User account’s Username and Password on the “Builtin Setup” screen during the install, do it now. Below are the steps to do this manually.

> **Important!** – This is the only way to access CMS400.NET if your Administrator accounts are locked. Make sure you change this to something that would be difficult for others to guess, but you will remember. If you don’t change this now, you can do so from the Workarea after the setup is complete.

1. Log into the Workarea as an Administrator by navigating to your Web site’s login page. If you completed the cms400min install and are accessing the site from the server, click **Start** > **Programs** > **Ektron** > **CMS400v76** > **cms400min Site**. If you are accessing the Web site from another system, enter the path to the login page in your browser.
   `http://<site root>/cms400min/CMSLogin.aspx`
   Replace `<site root>` with the site root of your Web site.

> **Important!** – Change the name of your login page before your site goes live. Do not use `CMSLogin.aspx`. By using a unique name for your login page, you will make it harder for non-authorized users to log in.

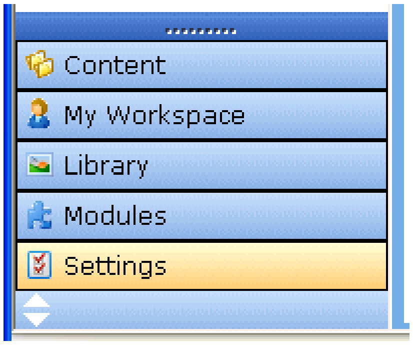


Enter your username and password.

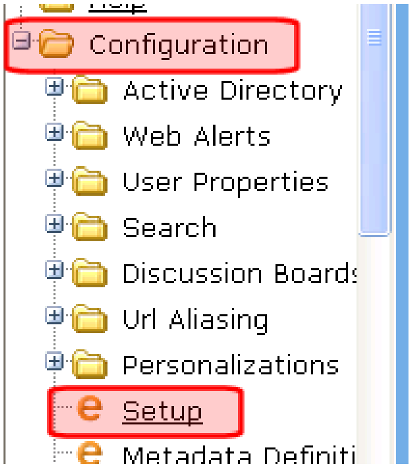
User: Admin

Pwd: ●●●●●

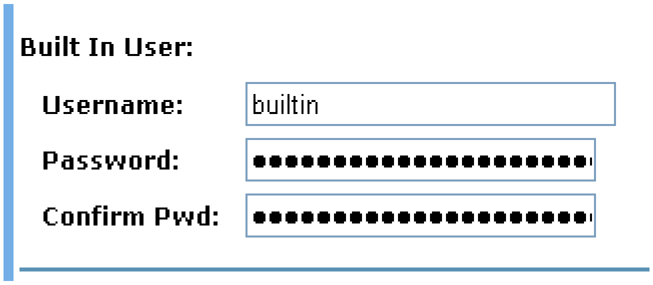
2. Once in the Workarea, click the **Settings** folder bar.



3. Click **Configuration** > **Setup**.



4. Once the Application Setup screen appears, click the **Edit** button ( ).
5. Scroll down to the **Built In User** area. (About half way down the page.)



Built In User:

Username: builtin

Password: ●●●●●●●●●●●●●●●●●●●●●

Confirm Pwd: ●●●●●●●●●●●●●●●●●●●●●

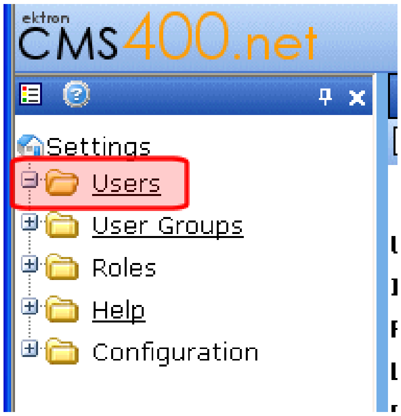
6. Change the username In the **Username** field.
7. Change the password in the **Password** field.
   Note: The new password must be at least seven characters long and use alphabetic and numeric characters.
8. Confirm the new password in the **Confirm Pwd** field.
9. Scroll back to the top of the page.
10. Click the **Save** button ( ).

> **Note**: If you forget your new Builtin username and password, you can use the BuiltinAccountReset.exe utility to reset the account. This is located in C:\Program Files\Ektron\CMS400v76\Utilities\BuiltinAccountReset

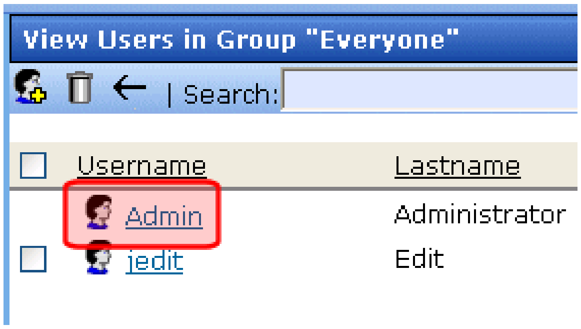
3.2.2.2 Change the Administrator's Username and Password

To do this:

1. Log into the Workarea using the default Admin Account.
2. Enter admin for the User.
3. Enter admin for the Password.
4. Once in the Workarea, click the **Settings** folder bar.
5. Click the **Users** folder.



6. Click **Admin**.



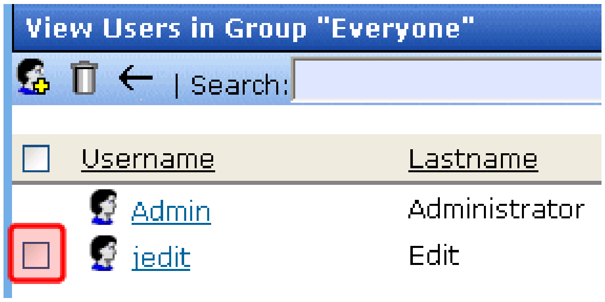
7. Click the **Edit** button ( ).
8. Change the username In the **Username** field.
9. Change the password in the **Password** field.

   Note: The new password must be at least seven characters long and use alphabetic and numeric characters.
10. Confirm the new password in the **Confirm Pwd** field.
11. Click the **Save** button ( ).

3.2.2.3 Remove the Demonstration User - jedit.

To do this:

1. Log into the Workarea as an Administrator.
2. Once in the Workarea, click the **Settings** folder bar.
3. Click the **Users** folder.
4. Click the check box next to jedit's username.


View Users in Group "Everyone"

Search:	

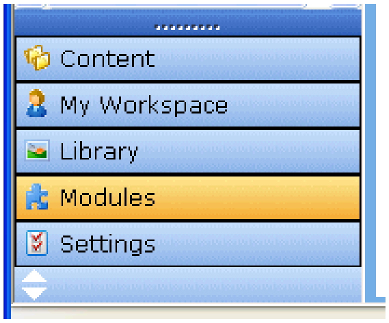
□ Username	Lastname
Admin	Administrator
□ jedit	Edit

5. Click the **Delete** button (🗑).
6. Confirm that you want to delete the user by clicking **OK** in the dialog box.
7. The page refreshes and the user is removed.

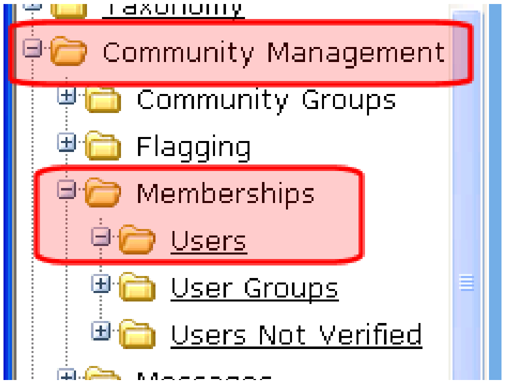
3.2.2.4 Remove the Demonstration Membership User - jmember

To do this:

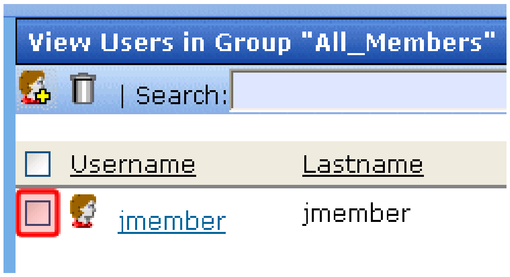
1. Log into the Workarea as an Administrator.
2. Once in the Workarea, click the **Modules** folder bar.



3. Navigate to **Community Management** > **Memberships** > **Users**.



4. Click the check box next to jmember's username.



5. Click the **Delete** button (🗑).
6. Confirm that you want to delete the membership user by clicking **OK** in the dialog box.
7. The page refreshes and the user is removed.

Note: If you are using a Starter Site other than cms400min for your Site Setup, remove or at least change the usernames and passwords on any Users or Membership Users included with the Starter Site.

3.3 Use 128 bit SSL Encryption

Using 128 bit SSL encryption on your CMS400.NET Web site is one of the most important things you can do to protect customers' credit card data. This protects a customer's credit card information when it's sent from a checkout Web page in their browser to your CMS400.NET server. It also allows for the encryption of the Workarea. This way, when an administrator or user with the Commerce Admin role logs into the Workarea, the information that is sent from their browser to the server and back is securely transmitted.

> **Important!** SSL certificates cannot be self-signed. They must be issued by a trusted certificate authority.

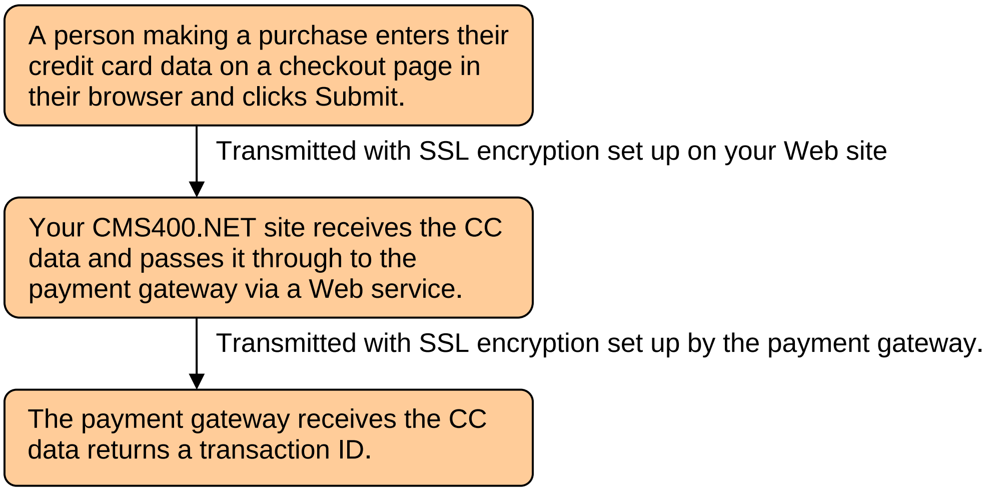
The following Microsoft article describes how to obtain, install, backup and manage SSL Certificates for IIS 6.0

- Obtaining and Installing Server Certificates (IIS 6.0)
- Backing Up Server Certificates (IIS 6.0)
- Managing Server Certificates Programmatically (IIS 6.0)

Once the SSL certificate is installed on your Web site, set the following keys in the Web.config file.

- Set the `ek_UseSSL` key to **"true"**
- Set the `ek_SSL_Port` key to the desired SSL Port.
  - By default, this is set to **"443"**, which is the port usually associated with secure web browser communications.
- Set the `ek_ecom_ComplianceMode` key to "**true"**
  - This enables encryption of the Workarea and logging of eCommerce actions.

Below is flow chart showing where the SSL encryption you install on your Web site is used during the purchase process.



A person making a purchase enters their credit card data on a checkout page in their browser and clicks Submit.

Transmitted with SSL encryption set up on your Web site

Your CMS400.NET site receives the CC data and passes it through to the payment gateway via a Web service.

Transmitted with SSL encryption set up by the payment gateway.

The payment gateway receives the CC data returns a transaction ID.

3.3.1 Using SSL Encryption with the Checkout Server Control

Ektron's Checkout server control allows a site visitor to navigate through the checkout process. A developer adds this control to a template when creating an eCommerce Web site with CMS400.NET. Part of this server control's purpose is to pass a user's credit card information to a payment gateway. Therefore, it is important to make sure an SSL certificate from a trusted certificate authority is installed for your Web site and that this control is using SSL encryption.

To have the Checkout server control use SSL encryption:

- Set the `IsSSLRequired` property on this control to **True**

3.4 Steps to Set up a Basic eCommerce Web Site

This section describes how to set up a basic eCommerce Web site. This walk through explains everything you need to set in the Web.config file and the Workarea. It also includes a list of templates needed and how to set up Ektron's eCommerce Server Controls on them.

Steps	**Description**

1. In the Web site's Web.config file, set the following keys:	`<add key="ek_ecom_DefaultCurrencyId" value="840" />`
	• this key determines the base currency for your Web site. The default is 840 (the US Dollar). If needed, change this to the Numeric ISO code for the default currency. **Important: Do not change this once the site is live.**
	`<add key="ek_MeasurementSystem" value="English" />`
	• this key determines how measurements are displayed on your site and in the Workarea. Change the value to "Metric" to use the Metric system. **Important: Do not change this once the site is live.**
	`<add key="ek_ecom_ComplianceMode" value="false" />`
	• set this key to "true" for your site to be Security Compliant. This means the Workarea will be encrypted in an SSL session and Logging is started. **Note:** If you chose to enable PCI Compliance during the install, this key is already set "True" **Important**: Setting this key to "true" requires you to have an SSL certificate install for your state.

	`<add key=“ek_ecom_PasswordHistory” value=“0” />`
	- set this key to “4” to force an administrator or user with the Commerce Admin role to have a password that does not match any of their last four passwords. A setting of “4” or higher is needed to achieve PCI DSS certification.
	
	`<add key=“ek_loginAttempts” value=“5” />`
	- set this key to “6” or less to lock out a user after he unsuccessfully tries to log in that number of times. A setting of “6” or lower is needed to achieve PCI DSS certification. By default, this is set to “5”.
	
	Depending on whether you are using IIS 6.0 or IIS 7.0 make sure the following line appears in the Web.config file. These lines are a part of the default install.
	
	In IIS 6.0, make sure this line appears between the `<httpModules>` tags.
	`<add name=“EkUrlAliasModule” type=“UrlAliasingModule” />`
	
	In IIS 7.0, make sure this line appears between the `<Modules>` tags.
	`<add name=“EkUrlAliasModule” type=“UrlAliasingModule” preCondition=“integratedMode” />`
	
	More Information:
	A list of currencies and their Numeric ISO code can be found in the Workarea > Modules > Commerce > Configuration > Currencies section. The ID is the Numeric ISO code.

2. Select a default Payment Gateway.	The following payment gateways are available for use with Ektron CMS400.NET. - Authorize.Net - PayPal’s Payflow Payment Gateway If you are going to work with one of these payment gateways, contact them to acquire account information, such as, user ID, password and any custom values that need to be passed to the gateway during a transaction. Once you have this information, select a gateway provider in the Workarea and input the information. To use one of the payment gateways shipped with CMS400.NET, you can set it in the Workarea. 1. Log into the Workarea as an Administrator. 2. Navigate to **Modules** > **Commerce** > **Configuration** > **Payment Gateway**. 3. Click a payment gateway’s name. 4. Click the **Edit** button. 5. Add your User ID, Password and any needed Custom Values. 6. Click the **Default** check box to make that selection the default. 7. Click the **Save** button.
3. Set up a shipping provider	If you are not using the default flat rate shipping provider, open the shipment.config file and set the default provider in formation in `<shipmentProvider defaultProvider=“FlatRateShipmentProvider”>` to either

	“FedExShipmentProvider” or “UPSShipmentProvider”. If you are using either of these shipping methods, make sure you fill in the following information in the <providers> tags. This information is provided by FedEx and UPS. (If you don’t see these items, scroll the window to the right.) • key=”” • password=”” • accountNumber=”” • meterNumber=””
4. Enable the Countries where your Web site will be selling its products. **Note**: The United States is enabled by default.	Enabling a country in CMS400.NET: • makes it available for site visitors to use it as part of an address for shipping and billing purposes • makes it available for use when you add a warehouse • automatically enables its corresponding tax table in the Country Tax Table section of the Workarea **Enable Countries in the Workarea.** 1. Navigate to **Modules** > **Commerce** > **Configuration** > **Countries**. 2. Click a country’s name. 3. Click the **Edit** button. 4. Click the **Enabled** check box. 5. Click the **Save** button. **More Information:** To learn about how Countries are used in CMS400.NET, see the Administrator Manual section “eCommerce” > “eCommerce Configuration Screens” > “Countries”
5. Add and enable Regions for each Country your eCommerce site will service.	Regions can represent states, provinces, territories, etc. and further define areas of a country. Adding and enabling regions: • makes it available for site visitors to use it as part of an address for shipping and billing purposes • makes it available for use when you add a warehouse • automatically enables its corresponding tax table in the Regions Tax Table section of the Workarea **Add Regions in the Workarea.** • Prerequisite: The region’s country is defined in the Countries screen. 1. Navigate to **Modules** > **Commerce** > **Configuration** > **Regions**. 2. Click **New** > **Region**. 3. Enter a Name. 4. Click the **Enabled** check box. 5. In the Code box, enter an abbreviation for this region. 6. Select this region’s country from the pull down list. 7. Click the **Save** button. **More Information:** To learn about how Regions are used in CMS400.NET, see the Administrator Manual section “eCommerce” > “eCommerce Configuration Screens” > “Regions”
6. Enable Currencies for your eCommerce	If your Web site is selling products in another country and you want to display prices in that country’s currency, enable it in the Workarea. 1. Navigate to **Modules** > **Commerce** > **Configuration** >

Note: By default, U.S. dollar, Euro and Australian dollar are enabled.	2. Click a currency. 3. Click the **Enable** button. 4. Set the Exchange Rate. **Note:** The default currency set in the Web.config file is the base reference currency when setting an exchange rate. 5. Click the **Save** button. **More Information:** To learn about how Currencies are used in CMS400.NET, see the Administrator Manual section “eCommerce” > “eCommerce Configuration Screens” > “Currencies”
7. Decide which credit cards you want your eCommerce site to accept.	Credit cards are used during the checkout process, by the Checkout server control, during the submit phase. During this phase, all enabled credit cards appear in a drop down which site visitors use to select their choice. **Add credit card types in the Workarea.** 1. Navigate to **Modules** > **Commerce** > **Configuration** > **Credit Card**. 2. Click **New** > **Credit Card Type**. 3. Enter the credit card’s name; for example, Visa. 4. Check the **Accepted** check box. 5. Add an image. 6. Add a Regex Expression to validate the credit card number. 7. Click the **Save** button. **More Information:** To learn about how Credit Cards are used in CMS400.NET, see the Administrator Manual section “eCommerce” > “eCommerce Configuration Screens” > “Credit Card Types” To learn about the Checkout server control, see “Checkout Server Control” on page 335.
8. Add and select shipping methods in the Workarea.	Once a shipping provider is set up (done in step 3), define the shipping options from which your site visitors can select. For example, if you use UPS, define whether to allow Next Day, 2nd Day, 3rd Day, Ground, World Wide Standard, etc. Once a Shipping Method is enabled, it will appear in the Shipping Method phase of the Checkout server control. **Shipping Methods are defined in the Workarea.** 1. Navigate to **Modules** > **Commerce** > **Shipping** > **Methods**. 2. Click **New** > **Shipping Method**. 3. Enter a Name. This name represents the option in the Shipping Method phase of the checkout server control. 4. Click the **Active** check box to enable this method. 5. Click the **View Options** link. 6. From the **Provider Service** drop down, select a shipping method. 7. Click the **Save** button. Repeat these steps until you’ve added all the necessary shipping methods. **More Information:** To learn about how Shipping Methods are used in CMS400.NET, see the Administrator Manual section “eCommerce” > “eCommerce Shipping Screens” > “Shipping Methods.”

9. Add a warehouse from which your products will be shipped.	This does not have to be the actual shipping address for the products. CMS400.NET uses this information to determine the “from” address when calculating shipping cost. **Add warehouse information in the Workarea.** 1. Navigate to **Modules** > **Commerce** > **Shipping** > **Warehouses**. 2. Click **New** > **Warehouse**. 3. Complete the address information fields. **Note:** Only countries and regions that have been enabled for eCommerce appear in the drop down lists. 4. Click the **Default Warehouse** check box if you want this to be the default warehouse. Only the default warehouse is used in the checkout process. 5. Click the **Save** button. **More Information:** To learn about how Warehouses are used in CMS400.NET, see the Administrator Manual section “eCommerce” > “eCommerce Shipping Screens” > “Warehouses.”
10. Define each package size your shipping department uses to ship your products. (Optional)	Tangible products in an order will have size and weight dimensions associated with them. CMS400.NET’s shipping calculator will use this information with the package size information to fit the order into the smallest-sized and fewest packages. It then passes packaging information (number, sizes and weight) to the shipping provider, which returns the order’s shipping costs. **Define package information in the Workarea.** 1. Navigate to **Modules** > **Commerce** > **Shipping** > **Packages**. 2. Click **New** > **Package**. 3. Enter a **Name**, **Length**, **Height**, **Width** and **Maximum Weight** a package can handle. 4. Click the **Save** button. Repeat these steps until you’ve added all the package sizes your company uses. **More Information:** To learn about how packages are used in CMS400.NET, see the Administrator Manual section “eCommerce” > “eCommerce Shipping Screens” > “Packages.”
11. Create Product Type definitions for each type of product you are selling. **Note:** This rest of the steps in this example will be based off selecting a Product for the Product Type Class.	Product types are applied to your catalog folders and allow you to control the way product information is added to a catalog. This concept is similar to the way Smart Form configurations are applied to content folders to control the way content blocks are created. You can apply multiple product types to a catalog. **Define product types in the Workarea.** 1. Navigate to Modules > Commerce > Catalog > Product Types. 2. Click New > Product Type. 3. Define the Product Type’s: • **Properties Tab -** Enter a Title and Description. Next, select a class. The Class represents the overall type of product that catalog entries will be based on. ▪ **Product -** typically a singular item. This selection also allows users to create a complex product where site

	▪ **Kit -** when you want to have a base product to which site visitors can add extra cost options. For example, you offer a computer kit and allow users to upgrade memory, CPU and hard drive. ▪ **Bundle** - used to combine several products under one umbrella selection. For example, you sell hat, mittens and a scarf as individual items and you want a catalog entry that also sells them as a set. ▪ **Subscription** - a product or service which site visitor receives and agrees to pay for over a period of time. For example, you could create a subscription to content on your site and charge a monthly fee. • **Attributes Tab** - (Optional) additional optional information applied to each Catalog Entry (product) using this product type. For example, you could create a year attribute using the Number selection. Then, when users create a new catalog entry, they can enter the year the product was made. This information is displayed when a site visitor views the product's details page. Click the **Add Attribute** button, enter a name and select an attribute type. **Note:** You can set a default for each attribute once it has been added to list by clicking the edit button. This will then become the default selection in a catalog entry's Attribute tab. ▪ **Text -** a user can enter free text into when defining a catalog entry's attributes tab. ▪ **Date -** a user can select a date to apply to a catalog entry's attributes tab. ▪ **Number** - a user can enter a numeric value to apply to a catalog entry's attributes tab. ▪ **Yes/No -** a Boolean value to apply to a catalog entry's attributes tab. • **Media Defaults Tab -** (Optional) enter the default image sizes to be generated when a user adds an image to the catalog entry's Media tab. For example, if you want to automatically create small and large images for each image a user adds, create a default in the appropriate pixel size. Click the **Add Thumbnail** button; enter a **Name**, **Width** and **Height**. Then click **OK**. 4. Click the **Save** button and move to the next step. **More Information:** To learn about defining product types, see the Administrator Manual section "eCommerce" > "eCommerce Products" > "Product Types."
12. Create the content page.	After clicking the Save button from the previous step, a content editor screen appears and allows you to enter XML Smart Form information. This Smart Form is what a user fills out when creating a Catalog Entry (Product). The information added by a user appears on a product's details page on your Web site. Here are some fields you might want to create in your smart form. • Title • Description • Image Once you have the Smart Form complete, click the Save button.

	More Information: To learn about defining Product Types, see the Administrator Manual section “eCommerce” > “eCommerce Products” > “Product Types.” To learn about Smart Forms, see the Administrator Manual section “Managing Content” > “Working with Smart Forms.”
13. Create a catalog and assign it a product type.	A catalog folder is a CMS400.NET folder designed to hold eCommerce entries (products). This is similar to the way content folders hold HTML or Smart Form content. By assigning a product type to the folder, you can control the way products are added to the catalog. **Catalogs are created in the Workarea.** 1. Click the Content folder bar to display the list of content folders. 2. Click **New** > **Catalog**. 3. Set the catalog’s Properties, Metadata, Web Alerts and Breadcrumb information. (Similar to creating a Content Folder.) 4. On the Product Types Tab, select a Product Type from the drop down list. 5. Click the **Add** link. 6. Click the **Save** button. **More Information:** To learn about Catalogs and assigning Product Types, see the Administrator Manual section “eCommerce” > “eCommerce Products” > “Creating a Catalog Folder” and in that section, see “Assigning a Catalog Folder’s Product Type.”
14. Add Catalog Entries to a Catalog.	Catalog Entries are the products you want to offer for sale on your eCommerce Web site. For example, a catalog entry could be a CD, a subscription based service, or a computer system that a site visitor can customize and the price adjusts accordingly. **Create catalog entries in the Workarea.** 1. Navigate to a catalog folder. 2. Click **New** and select a product type. 3. In the **Title** field, enter a name for the catalog entry. 4. Fill out the fields in the Smart Form as necessary. 5. Select the **Summary** tab and add a summary. (Optional) 6. Select the **Properties** tab and enter an SKU and the number of units that equal one purchase. Next, select a Tax Class. If the product is a tangible product, click the Expand link next to Dimensions, click the Tangible check box and enter the product’s physical dimensions. If you are using CMS400.NET as your inventory system, click the Expand link next to Inventory and enter the information. 7. Select the **Pricing** tab and enter the product’s list price and sales price. If you are offering a quantity discount, click the **Add Pricing Tier** button and add a quantity and a tier price. If you enabled multiple currencies, select a currency from the drop down and add pricing information as needed. 8. Select the **Attributes** tab and fill-out or change attributes as needed. **Note:** If you did not define attributes, the Attributes tab does not appear. 9. Select the **Media tab** and click the **Add Images** button to associate images with the catalog entry. 10. Enter information as needed on these tabs: Metadata, Taxonomy and Schedule. 11. Click **Action** > **Publish**.

	More Information: For information on creating catalog entries, see the Administrator Manual section “eCommerce” > “eCommerce Products” > “Creating a Catalog Entry.”
15. Overview Create the Web site templates your site visitors will use to interact with your eCommerce site.	Here is a list of the templates needed to create a basic eCommerce site. • **Master page -** recommended, but not absolutely necessary. This template could contain any of the following: ▪ CurrencySelect server control - allow site visitors to choose a currency. ▪ View Cart link - links to the template containing the Cart server control. ▪ View My Account / Orders link - links to the template containing the MyAccount and OrderList server control. ▪ Login server control - allows site visitors and users to log in from any page. • **Landing page -** this page should have a way for site visitors to start the shopping process and could contain a ProductList, ProductSearch server control. • **Product Display page -** use the Product server control on a template to display the details of a catalog entry (product). If you are using the Cross Sell or Up Sell functionality, add a recommendation server control to this template. • **Product Search page -** use the ProductSearch server control on a template to allow site visitors to search for product. • **Cart page -** use the Cart server control on a template to allow a site visitor to work with the items they have selected to purchase. • **Checkout page -** use the Checkout server control on a template to facilitate the check out process. • **My Account / Order History page -** use a MyAccount server control and an OrderList server control to display a site visitor’s account information and a list their order history. The rest of the steps below are an example of creating a Web site using Ektron’s eCommerce Server Controls.
16. Create a Master page.	Create a master page and add the following items to a header area or left side column. • **CurrencySelect Server** C**ontrol -** allows site visitors to select from available monetary types. This control displays the currencies that were enabled earlier. • A **MyCart link** that leads to a template containing the Cart server control. • **My Account / Order History link** that leads to a template containing the MyAccount and OrderList server controls. • **Product Search link -** (optional) add a link that leads to a template containing a ProductSearch server control. • **Product Search Server Control -** (optional) allows a user to search for a product from anywhere on the site. Note: Adding this option is involves more than just dragging and dropping a server control to the header or the left side column, it includes some advanced customizations and coding that allows the search term to be passed from one form to another. Ektron’s Developer Sample site shows an example of doing this with the WebSearch server control.

	• **Login server control** - (optional) this allows existing customers to login once they arrive at your site. If you only want site visitors logging in through this control, set the OnlyAllowMemberLogin property to True. For more information on the server controls mentioned in this step, see the Developer Manual’s eCommerce Server Control section.
17. Create a Landing page.	This template should be the first page a site visitor sees when they arrive at your site and it should have a way for site visitors to start shopping for product. Make sure this page has one of the following: • **ProductList server control** - use this control to display products by Taxonomy, Catalog or ID. ▪ To display a single taxonomy, set the SourceType property to Taxonomy and enter a single Taxonomy ID in the SourceId property. ▪ To display multiple taxonomies, set the SourceType property to TaxonomyList and enter a comma separated list of Taxonomy IDs in the IdList property. ▪ To display a single catalog, set the SourceType property to Catalog and enter a single catalog ID in the SourceId property. If you want to display sub catalogs for a given ID, set the Recursive Property to True. ▪ To display multiple catalogs, set the SourceType property to CatalogList and enter a comma separated list of catalog IDs in the IdList property. ▪ To display products by their ID, set the SourceType property to IdList and enter a comma separated list of product IDs in the IdList property. ▪ Set the TemplateProduct property to the template containing the Product server control. • **ProductSearch server control** - this control provides the means for site visitors to search your Web site for products. If this control is not on your landing page or part of your master page, you should create a separate template containing this control. ▪ Set the CatalogId property to the ID of the catalog to search. ▪ Set the TemplateCart property to the template containing the Cart server control. ▪ Set the TemplateProduct property to the template containing the Product server control. For more information on the server controls mentioned in this step, see the Developer Manual’s eCommerce Server Control section.
18. Create a Product page	This is the template where a site visitor views a product’s details. It contains a Product server control and optionally a Recommendation server control. • **Product server control** - this control displays a product’s details. ▪ Make sure the DynamicParameter property is set to the parameter name used to pass product IDs to the QueryString. ▪ If you want a default product to display when no ID is passed, set the DefaultProductID property to the ID of a product. ▪ Set the TemplateCart property to the template containing the Cart server control.

	• **Recommendation server control -** this control displays Cross Sell and Up Sell opportunities associated with a product. These are set in Workarea, under the View menu’s Cross Sell and Up Sell selections for a catalog entry. ▪ Set the RecommendationType property to CrossSell or UpSell. ▪ Make sure the DynamicProductParameter property is set to the parameter name used to pass product IDs to the QueryString. ▪ If you want a product’s default Cross Sell or Up Sell items to display when no ID is passed, set the DefaultProductID property to the ID of a product. ▪ Set the TemplateCart property to the template containing the Cart server control. ▪ Set the TemplateProduct property to the template containing the Product server control. For more information on the server controls mentioned in this step, see the Developer Manual’s eCommerce Server Control section.
19. Create a Product Search page.	This page allows site visitors to search for products on your Web site. • **ProductSearch server control** - this control provides the means for site visitors to search your Web site for products. If this control is not on your landing page or part of your master page, you should create a separate template containing this control. ▪ Set the CatalogId property to the ID of the catalog to search. ▪ Set the TemplateCart property to the template containing the Cart server control. ▪ Set the TemplateProduct property to the template containing the Product server control. For more information on the server controls mentioned in this step, see the Developer Manual’s eCommerce Server Control section.
20. Create a Cart page.	This template contains a Cart server control. • **Cart server control** - this control allows a site visitor to work with products they have selected to purchase. As a site visitor navigates around your site selecting products to purchase, they are added to a cart. ▪ Set the TemplateCheckout property to the template containing the Checkout server control. ▪ Set the TemplateProduct property to the template containing the Product server control. ▪ Set the TemplateShopping property to the Landing page template or a template containing a ProductList or ProductSearch server control. ▪ If you are using coupons make sure the EnableCoupons property is set to True. For more information on the server controls mentioned in this step, see the Developer Manual’s eCommerce Server Control section.
21. Create a Checkout page	This template contains a Checkout server control. • **Checkout server control -** this control allows a site visitor to navigate through the checkout process. ▪ Set the DefaultCountryID property to the country you

	▪ Set the TemplateCart property to the template containing the Cart server control. ▪ Set the TemplateOrderHistory property to the template containing the OrderList server control. ▪ Set the TemplateShopping property to the landing page template or a template containing a ProductList or ProductSearch server control. ▪ Set the IsSSLRequired property to True. For more information on the server controls mentioned in this step, see the Developer Manual's eCommerce Server Control section.
22. Create a My Account page.	This template contains a MyAccount and an OrderList server control. • **MyAccount server control** - this server control allows site visitors to view billing, shipping and alternative shipping information associated with their account. ▪ Set the DefaultCountryID property to the country you want to be the default selection in the Billing and Shipping address sections. • **OrderList server control** - this server control allows site visitors to view a list of their processed orders. ▪ Make sure the DynamicOrderParameter is set to the parameter name used to pass order IDs to the QueryString. ▪ Make sure the DynamicProductParameter is set to the parameter name used to pass product IDs to the QueryString. For more information on the server controls mentioned in this step, see the Developer Manual's eCommerce Server Control section.

3.5 Test Your Payment Gateway

Make sure you test transactions to your payment gateway. Most payment gateway providers have an alternative gateway you can use to test payment transactions from your site. If you are using one of the included payment gateways, enable test mode in CMS400.NET. To do this:

- Set the `ek_ecom_TestMode` key to "true" in the site's web.config file.

When set to true, the payment gateway provider's test gateway is used. Once you are satisfied that transaction are being handled properly and the payment gateway is properly configured, set this key to false.

> **Important!** Never use actual live cardholder data when testing your payment gateway. Typically, your credit card processor can provide you with test cardholder data.

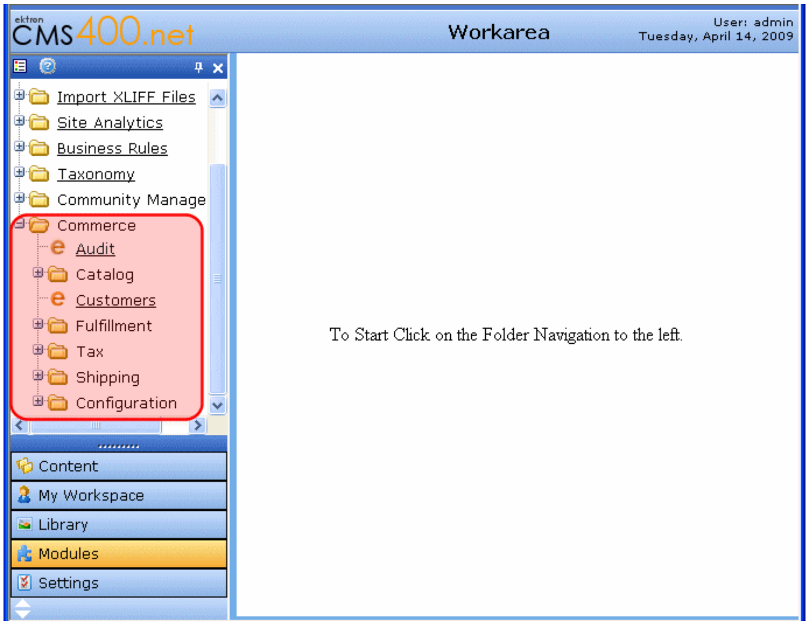
3.6 Administrators vs. the Commerce Admin Role

Make sure your administrators understand the ramifications of giving another user full administrator privileges. If a user needs to perform eCommerce tasks in the Workarea, they should be added to the Commerce Admin Role. See the Ektron CMS400.NET Administrator Manual section "Managing Users and Permissions" > "Defining Roles" for information on how to define roles in CMS400.NET.

3.7 Understanding Ektron CMS400.NET in an eCommerce Environment

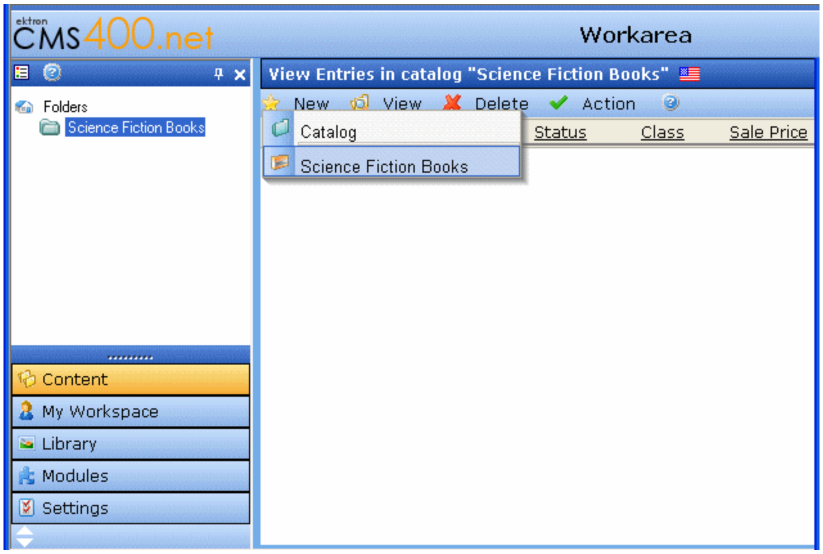
Make sure you understand all the following areas of CMS400.NET:

- **Workarea eCommerce screens** – these screens are described in the CMS400.NET Administrator Manual “eCommerce” section. To view these screens in the Workarea, navigate to **Modules** > **Commerce**.



To Start Click on the Folder Navigation to the left.

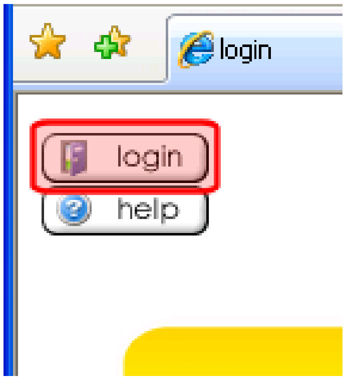
- **How content editors create product content for your site** – this is described in the CMS400.NET Administrator Manual “eCommerce” > “eCommerce Products” section. Editors add product content in a Workarea Catalog folder.

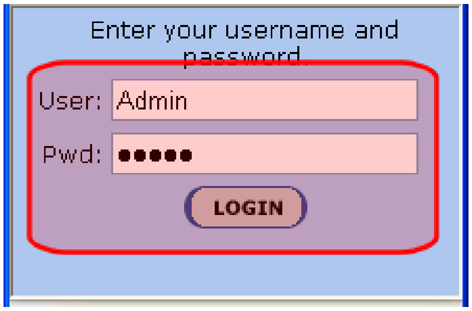


- **How administrators, users and membership users are created and the difference between them** – this information is described in the CMS400.NET Administrator manual “Managing Users & User Groups” > “Managing Users & User Groups” section and the “Membership Users and Groups” section.
  - To view a user’s account information in the Workarea, navigate to **Settings** > **Users**.

  - To view a membership user’s information in the Workarea, navigate to **Modules** > **Community Management** > **Memberships** > **Users**

- **How to log into your CMS400.NET Web site** – log into your site by navigating to your Web site’s login page.




Enter your username and password.

User: Admin

Pwd: ●●●●●

3.8 Train Your Personnel

Training the people who run your site is an important part of running a successful an eCommerce Web site. This can include the following personnel: Administrators, User with the Commerce Admin Role, Web site Developers, Content Editors and Quality Assurance team members. It is your responsibility to train these people. Here are some suggestions to help train your personnel.

- Ektron Developer, Administrator or End User training
- Information from this document
- Ektron’s CMS400.NET eCommerce Quick Start documentation
- Information from the PCI DSS compliance document