

**The TimeIPS
IPSSSEC
Enterprise
Enhanced Security
Module™**

- Encrypted data communications between all TimeIPS clocks
- Secure (HTTP SSL) site login and administration.
- Highest level Secure Socket Layer (SSL) encryption utilizing AES block cipher
- Ability to generate high security 1024-bit RSA encryption key certificates

FOR MORE
INFORMATION OR TO
PURCHASE THIS
MODULE
CONTACT TIMEIPS:
877-846-3256
sales@timeips.com
OR VISIT
www.timeips.com



**TimeIPS IPSSSEC
Enterprise Enhanced Security Module™**

The Must-Have Module For Security Minded Companies!

Don't leave the security of your system information to chance. In today's world it pays to ensure that no one but can access the sensitive information stored in the your TimeIPS system except the people you grant access to. Ensure that security today with cost-effective module.

Product Description

The TimeIPS IPSSSEC – **Enterprise Enhanced Security Module™** - is an essential addition to your TimeIPS suite if the security of your network is a high priority. This value-added module provides features such as secure site log-on and administration, highest level SSL encryption utilizing AES block cipher and the ability to generate high security 1024-bit RSA encryption key security certificates. You also get enhanced firewall protection.

Key Benefits of IPSSSEC™

- Encrypted data between all TimeIPS clocks – the data from the client clock(s) to the master clock is encrypted before transport within the system.
- Secure (HTTP SSL) site login and administration – Provides an additional encryption/authentication layer for restriction of access to only authorized users.
- Highest level Secure Socket Layer (SSL) encryption utilizing AES block cipher – Gives your data high security encryption to ensure the privacy of your data.
- Ability to use your own signed certificate, or generate a high security 1024-bit RSA encryption key certificate. (For web browsers to automatically recognize your SSL certificate, you must pay to have it be signed by an external authority.) The certificate administration feature of IPSSSEC™ allows your to select your certificate or create a new certificate.
- Enhanced firewall protection – Firewall protection is enhanced so that only recognized encrypted TimeIPS packets are allowed through the firewall into the system.



TimeIPS IPSSEC Enterprise Enhanced Security Module™

Key Features of IPSSEC™

Create a signed security certificate

- Enter your organization's information or click on the Browse buttons to select your Certificate and Private Key

Create a New Certificate or Install an Existing Certificate	
Generate Self Signed Certificate or Certificate Signing Request (CSR)	
Organization Name: <i>For example, the name of your company.</i>	<input type="text" value="Keeler Co."/>
Common Name: <i>This is the IP address or domain name used to access TimeIPS. If this is incorrect, your web browser may not accept the certificate.</i>	<input type="text" value="asp.timeips.com"/>
City:	<input type="text"/>
State or Province (Full Name): <i>Use the full name of your state or province, NOT an abbreviation.</i>	<input type="text"/>
Country Code: <i>Use the two-letter code for the country your TimeIPS® server is in. For example: US, CA, UK</i>	<input type="text" value="US"/>
E-Mail Address:	<input type="text" value="mkeeler@timeips.com"/>
Expiration: <i>How long your certificate will remain valid, in days. We recommend 3650 days (10 years).</i>	<input type="text" value="3650"/> days
Install Existing Certificate	
Install Your Own Certificate: <i>If you already have a signed X.509 certificate you wish to use, you may upload it here. The certificate and private key may not be encrypted with a password, they must be in PEM format, and they must have the address of the TimeIPS® server as their common name. If you provide a certificate, the fields above will be ignored.</i>	Certificate: <input type="button" value="Browse..."/> No file selected.
	Private Key: <input type="button" value="Browse..."/> No file selected.
	Chain File:(optional) <input type="button" value="Browse..."/> No file selected.
<input type="button" value="Generate/Install Certificate"/> and Enable Security	



Security Administration

Certificate Administration	
Certificate Information	
Organization Name:	Keeler Co.
Locality:	Wichita, Kansas, US
Common Name:	asp.timeips.com
E-Mail Address:	mkeeler@timeips.com
Valid Between:	Feb 05, 2014 12:30 pm CST Feb 03, 2024 12:30 pm CST
Signing Authority	
Organization Name:	Keeler Co.
Locality:	Wichita, Kansas, US
Common Name:	asp.timeips.com
E-Mail Address:	mkeeler@timeips.com
<input type="button" value="Revoke Certificate"/> and Disable Security	

FOR MORE INFORMATION OR TO PURCHASE THIS MODULE
CONTACT TIMEIPS BY PHONE: 877-846-3256 OR E-MAIL: sales@timeips.com
OR VISIT www.timeips.com