

Lecture. #10

Secure Online Shopping and Cybersecurity Standards



Dr. Redhwan M. A. Saad

Head of Cybersecurity Department

Faculty of Informatics

Midocean University



CyberSecurity Fundamentals (CYB670)



Secure Online Shopping and Internet Browsing

Introduction

HTTP Protocol
Websites

Secure Electronic
Transactions
(SET)

Web Fraud
Detection
Systems

Browser Cache
Clearing

Frequent
Password
Changes

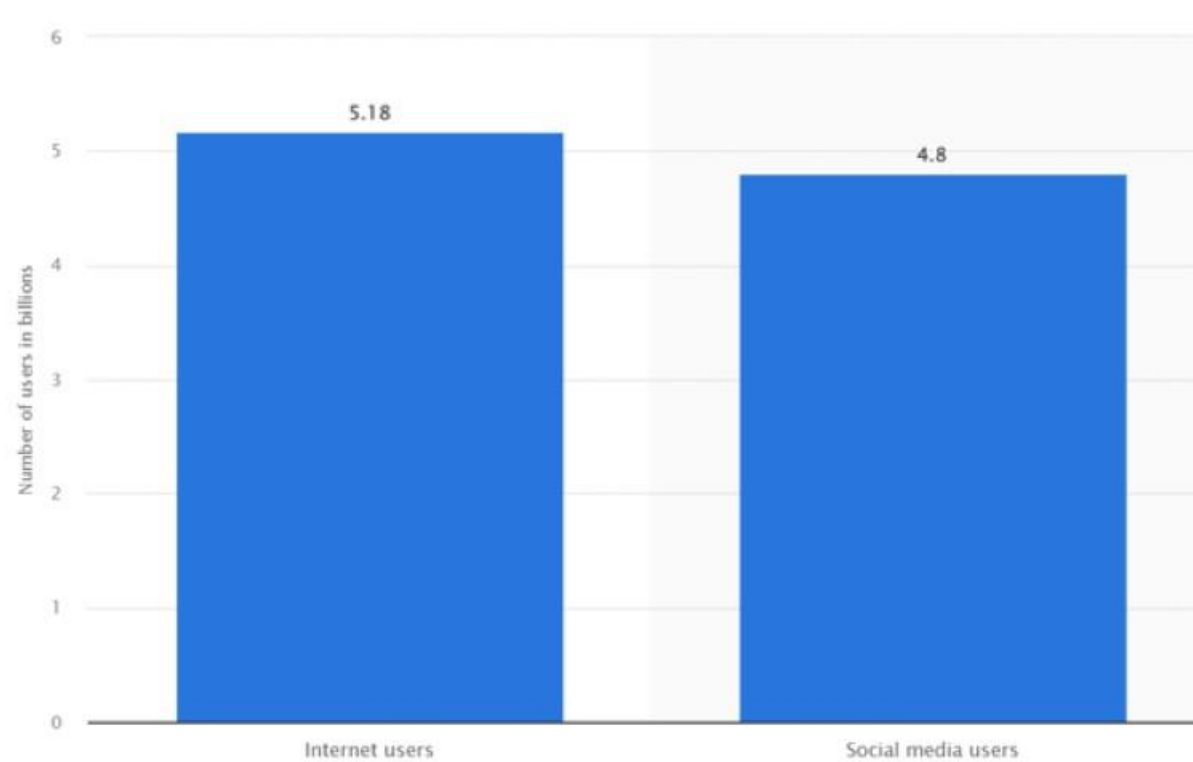
Updating OS

Updating Apps

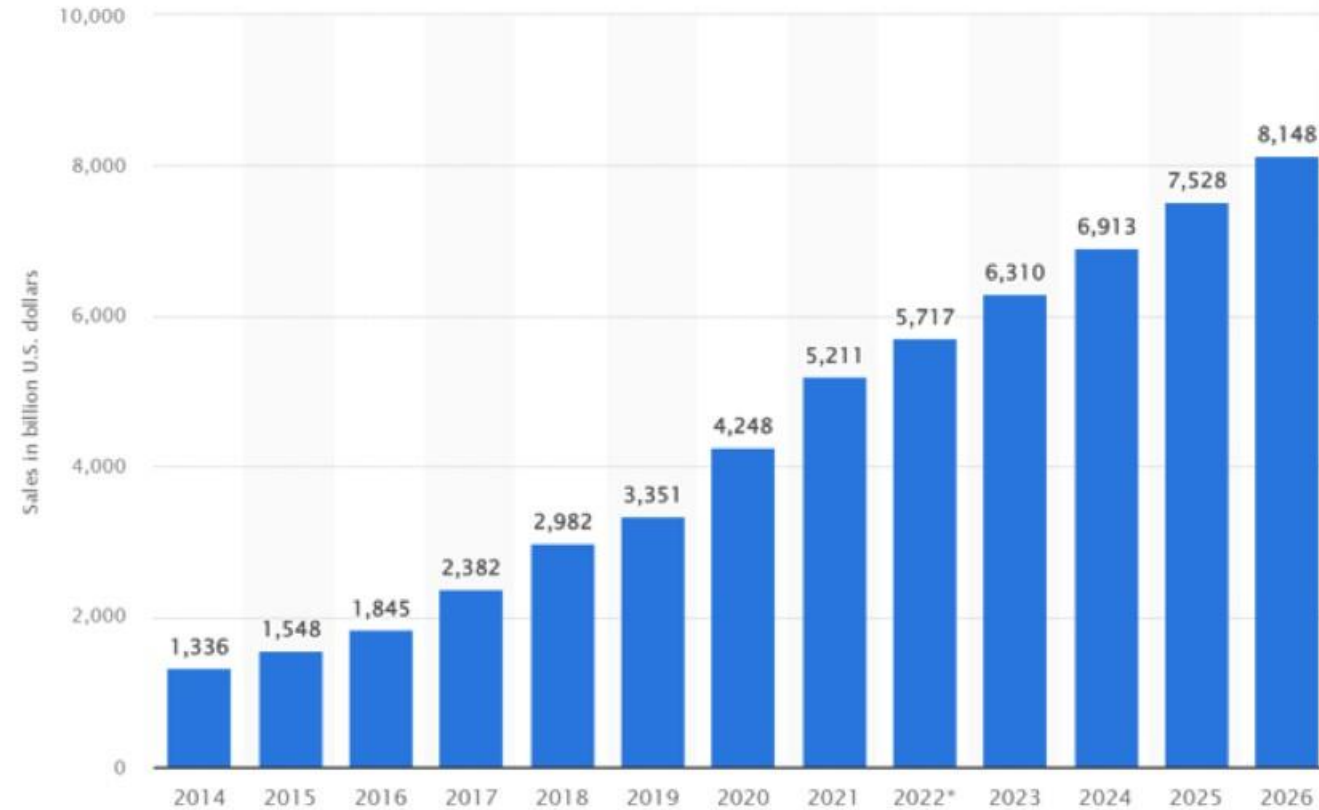
Useful Tips on
Safe Browsing &
Online Shopping



- Total global sales through e-commerce amounted to as much as \$ **\$6.33 trillion** trillion in **2024**, according to the Statista information. It is expected to cross the **\$7** trillion mark by **2025**. The increase in the online shopping is gigantic and it will keep growing for many years to come.
- Meanwhile, the number of internet users has increased tremendously across the globe. As of April 2023, there were **5.18 billion internet users worldwide**, which amounted to **64.6 percent** of the global population. Of this total, **4.8 billion**, or **59.9 percent** of the world's population, were social media users.
- With this huge digital population of the world, the volume of both risk and opportunity has increased tremendously. The biggest risk for this huge digital population is the cybercrimes.



Number of internet and social media users worldwide as of April 2023 - [© Statista 2023](#)



Retail e-commerce sales worldwide from 2014 to 2026 [© Statista 2023](#)



- It is very important to note that **cyber criminals are highly creative**, technically sound, and cunning. They exploit every aspect of an online user including the way he/she uses the internet, types of tools, financial credentials, personal information, and many others things.
- According to the FBI Internet Crime Complaint Center, more than 300 thousand complaints were received in 2017 regarding the online crimes. The total cost of those criminal activities amounted to about \$1.4 billion to the complainants in 2017 in the USA only.
- So, it is highly recommended to all necessary measures related to the online shopping and internet browsing to keep the digital criminals at bay.



The main points that are normally exploited by the cyber criminals include the following:

- Introduction of poisonous links by using the black SEO
- Malicious links and emails for phishing purpose
- Text messages and popup notifications
- Identity theft techniques
- Social engineering methods
- Software vulnerabilities to send virus, Trojan horse, and worms
- Operating system vulnerabilities
- Vulnerabilities in browsers
- Fake websites and offers
- Exploit your personal information that you provide
- Rogue and public access point vulnerabilities
- Use of weak passwords
- And yes, your carelessness
- Bad password management

So always take special care while shopping online or even browsing the internet and follow the security guidelines to avoid any cyberattack on you.





The major things and activities that will help you enjoy the secure online shopping and internet browsing.



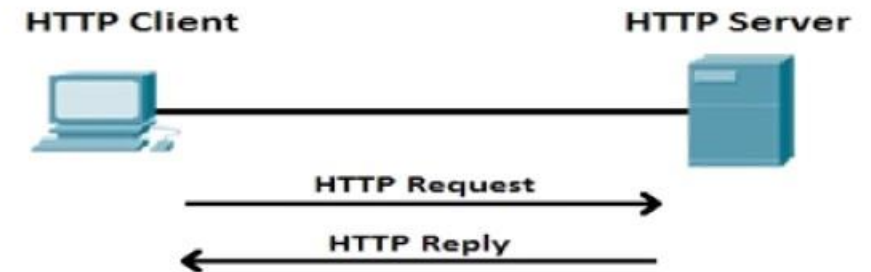
- HTTPS Protocol Websites
- Secure Electronic Transactions (SET)
- Web Fraud Detection Systems
- Browser Cache Clearing
- Frequent Password Changes
- Updating OS
- Updating Apps
- Useful Tips on Safe Browsing & Online Shopping



- Initially, the websites used the HTTP protocol for the communication between **server and client**. **The web browsers** are normally the **clients** of HTTP communication and **the web server applications** are the **server** of this communication.
- HTTP protocol** is considered as **insecure** nowadays because of the nature of **plain text** communication between client and server over the internet.
- The use of HTTP protocol has been replaced by the **HTTPS or HTTP (secure) protocol**, which include the capabilities of **encrypted** communication between server and client over the communication link.



- **HTTP protocol** can easily be converted to the **HTTPS protocol** by adding the **Secure Socket Layer SSL** encryption protocol. We will describe the step by step method on how to install SSL certificate to convert the HTTP protocol to HTTPS on the websites later in this section too. Before that, let's explain the HTTP protocol in detail.
- **Hypertext Transfer Protocol** precisely HTTP is an application layer communication protocol that is used for establishing the **internet communication between client and server**. A client is any software browser that is used to send the request for accessing certain resources located on the web server.
- The web server has the sever part of the HTTP protocol that provides response to the requests originated from the HTTP client.





The communication transactions of HTTP client/server are listed below:

- Client (web browser) sends HTTP request to server
- Server takes the request and starts app to process HTTP request
- Generates and sends back the required response requested by the client
- Client receives the response to display on the browser

In this request/response communication client can request for the website (HTML) page, database, JavaScript file, JPG images or style sheets. The response of the server will include the HTML files, JSON/XML files, JS files, JPG file or CSS files.





Let's talk about the following versions of HTTP related security protocols:

- Hypertext Transfer Protocol Secure (HTTPS)
- Installing Security Certificate on Windows IIS Server (See appendix)
- How SSL Encryption Works?



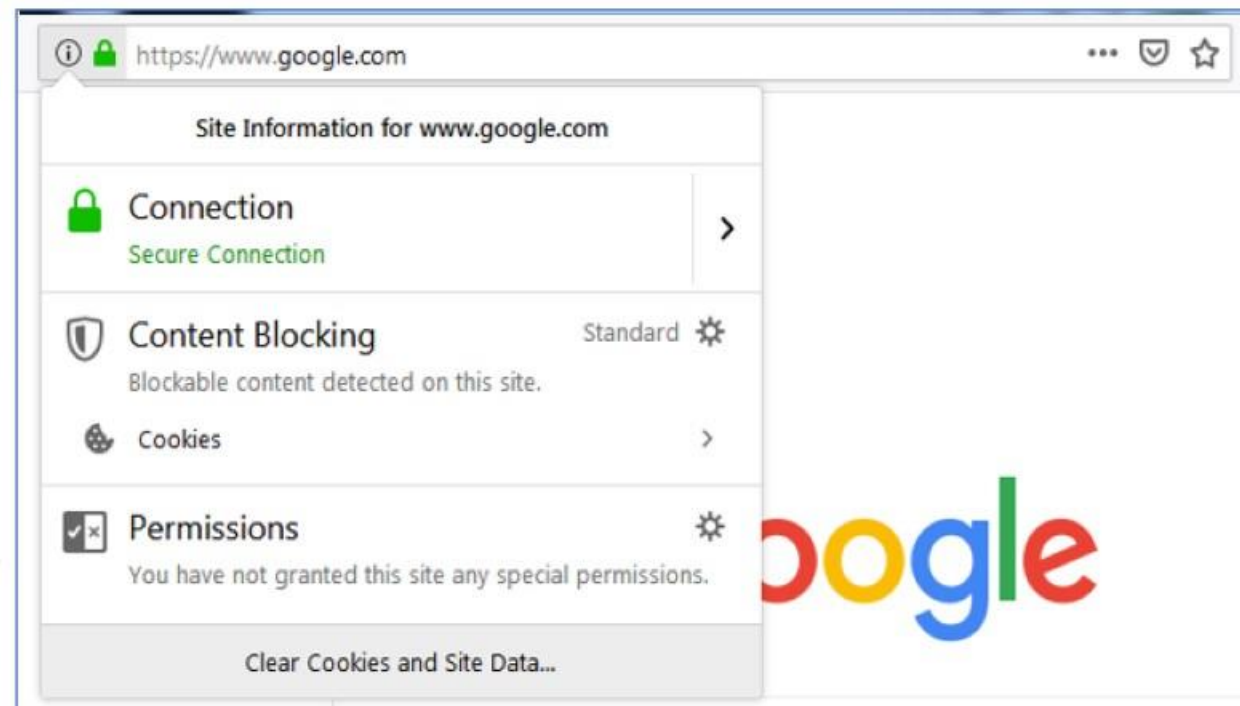
- If you use the HTTP protocol on your website, then the data you receive and send is transported is subject to external threats like **Man in The Middle (MITM) attacks, eavesdropping** of the communication and credential theft etc.
- For secure online shopping and internet browsing, **HTTPS** protocol-based websites should be used to prevent any cyber-criminal activities.



The website that uses HTTPS protocol and is secure to surf and shop can be **identified** by the following marks:

- The address bar shown **HTTPS://**
- A lock  sign appears on the address bar before website URL

To know details about the website security, click either lock  icon in Google Chrome or  symbol in Mozilla Firefox on the address bar. The details appear as shown in the image.



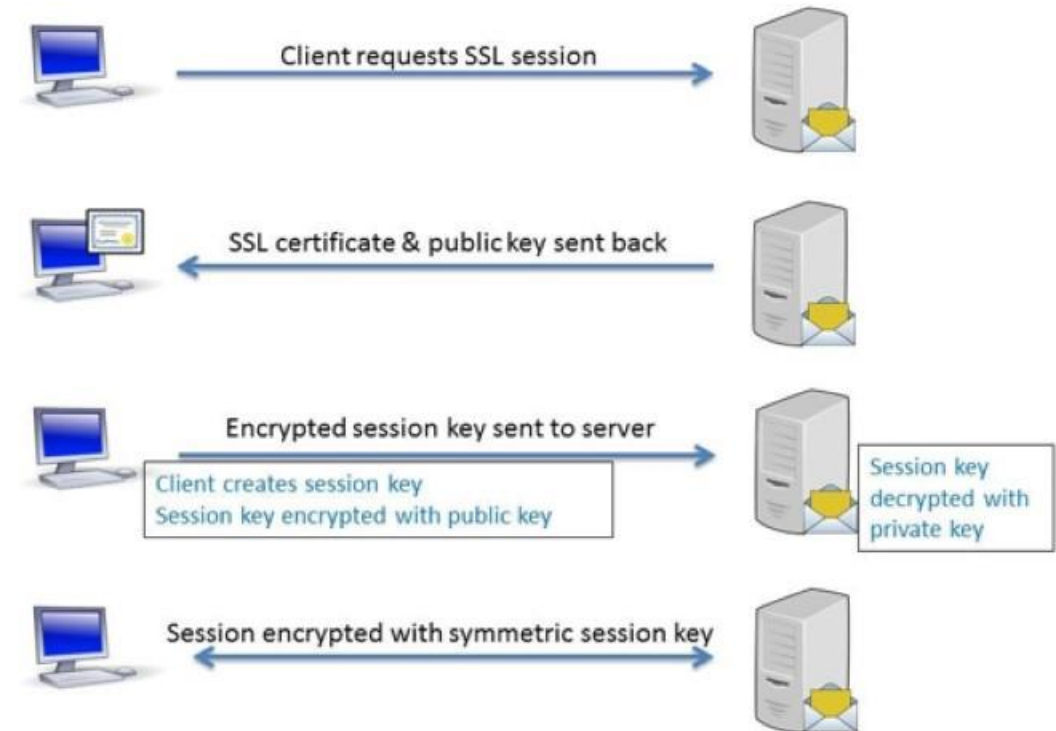


▪ How SSL Encryption Works?...

The domain name bound with the desired certificate will create a **socket layer** of communication between the supported browsers and the website communication port number **443**. The secure communication between a web browser and website through SSL communication socket takes place in the following steps:

- Browser sends the HTTP request to prove the SSL/TLS certificate targeting 443 port on the web server
- The website server sends response with the certificate chain, which includes the primary certificate, intermediate certificate and root certificate of the certificate authority
- All browsers have public keys and related information of all certificate authorities (CAs)
- Compares with the information with the local SSL information to verify the certificate

SSL Handshake Process





▪ How SSL Encryption Works?...

- When the public key of the server is verified in terms of validity and authority, it sends the its own public key to the server
- On the basis of public key received from browser and the private key of the server, an encrypted message will be created and sent out through port 443 to the browser
- The browser decrypts the message with the help of public key
- Thus, the communication over SSL link starts

It is important to note that encrypted transmission of data over the internet is becoming the fundamental requirement for safe browsing of the internet. Any website without encryption is considered as risky for the security of your data and system.



- **Secure Electronic Transactions (SET)** is a comprehensive communication protocol for maintaining the full security of the **online payments and financial transactions**
- **SET** is a consolidated online financial transaction protocol to carry out the secure online transactions such as online shopping, online bill payment, money transfer, and others





▪ Main features of SET technology ...

SET technology was developed to offer the full security to the valuable data, personal information, and bank authorization. The main features of SET protocol are listed below:

- Maintains high-level of personal information confidentiality
- Maintains high-level data integrity
- Incorporates merchant authorization
- Incorporates the authentication of cardholder's account
- Uses dual-signature mechanism for authentication and authorization
- Uses separate message digest DM algorithms for order information and payment information
- Powered by a large number of financial organizations





Web Fraud Detection System (WFDS) is a software-based system, which uses the latest technologies such as artificial intelligence and the latest scoring methodologies to find out the authenticity of the transaction.





▪ What algorithms are used in WFDS Systems? ...

Web fraud detection system WFDS is a software system, which uses the latest software technologies for detecting the fraudulent transaction. It uses the scoring system, which scores the transactions with the help of some algorithms known as the **scoring algorithms**. The main scoring algorithms used by the WFDS systems are listed below:

- Predictive Behavioral Scoring Model
- Rule-Based Scoring Model
- Hybrid Scoring Model

These scoring methods use the user behavior, using pattern or both pattern and behavior are used collectively to assess the web transactions.



- Normally, all types of browsers cache the information about the browsing history, browsing information like forms, data, and other information that you browse through.
- The browsers save certain forms and data retrieved from the online sources. **Those forms and offline data saved in the browsers cache memory load**, when you visit the related URLs. You can also load those resources offline, if saved for that purpose.

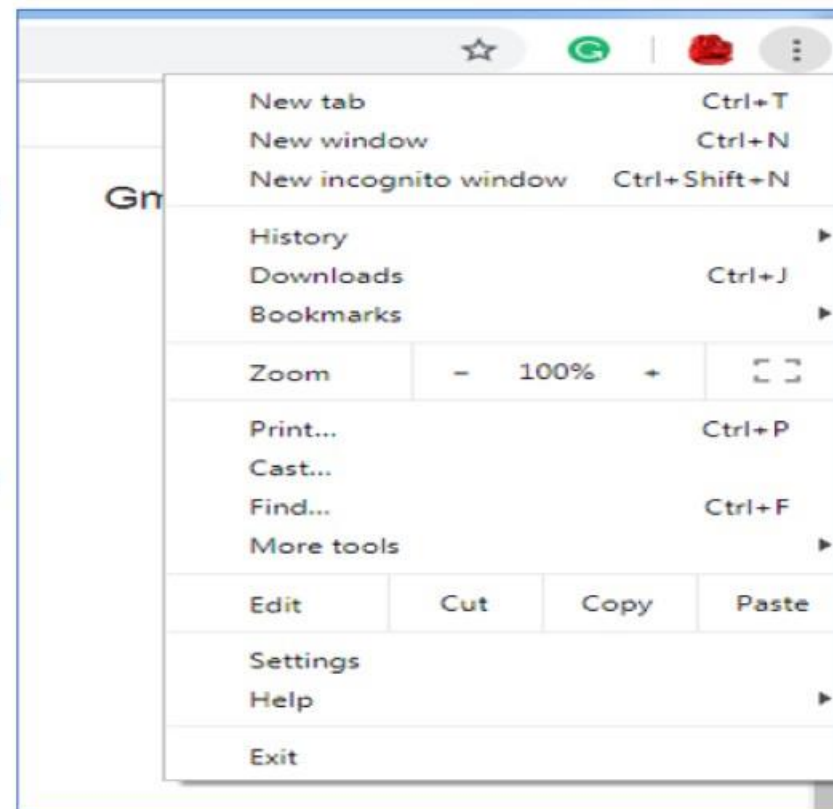




■ Google Chrome...

To clear the cache of Google Chrome browser, take the following steps.

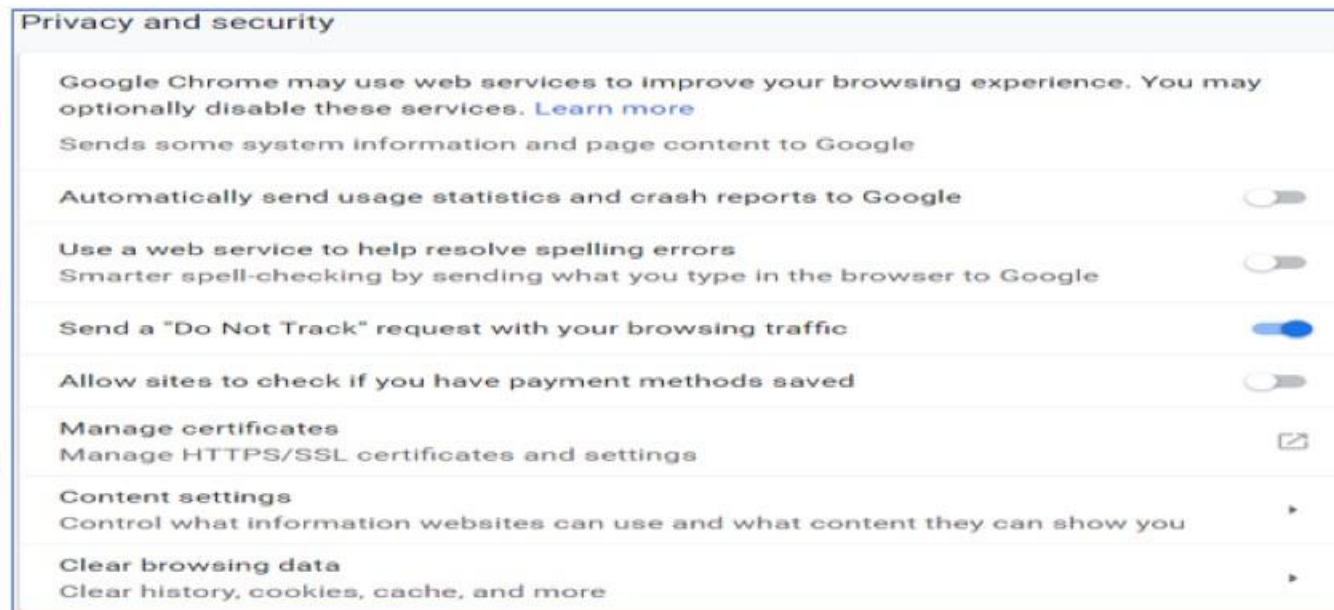
- Run the Google Chrome browser
- Click the  symbol located at the right corner of the screen. The list of the options appears as shown .





■ Google Chrome...

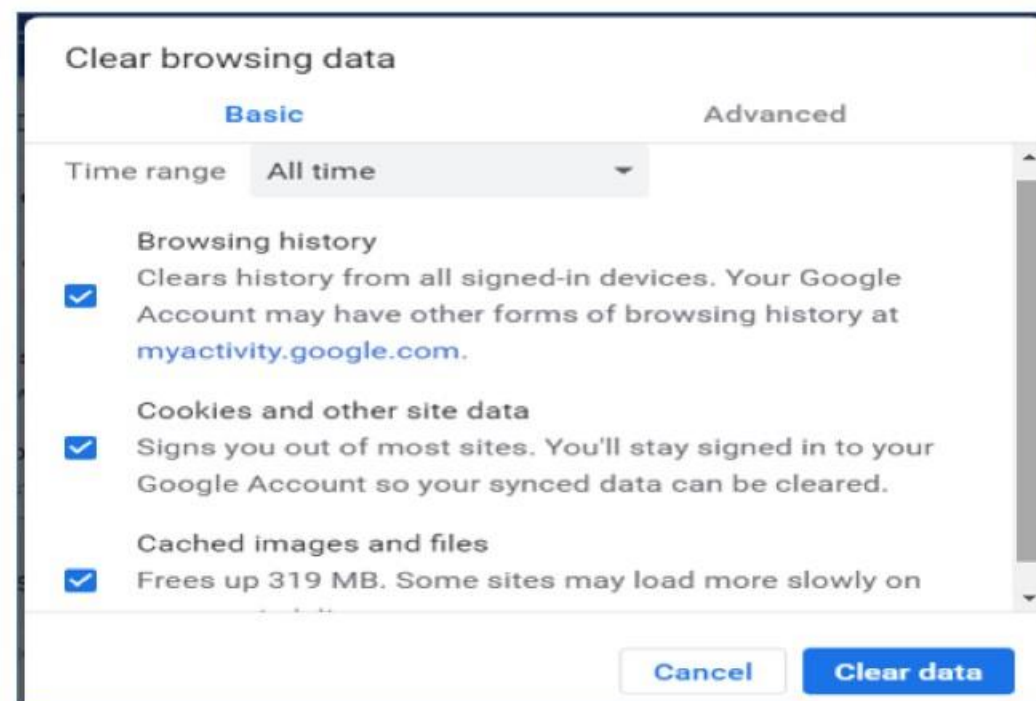
- Click the **Settings** option from the list. The **Setting** page appears.
- Scroll down to the **Advanced** option and click it.
- **Privacy and Security** category appears as shown below





■ Google Chrome...

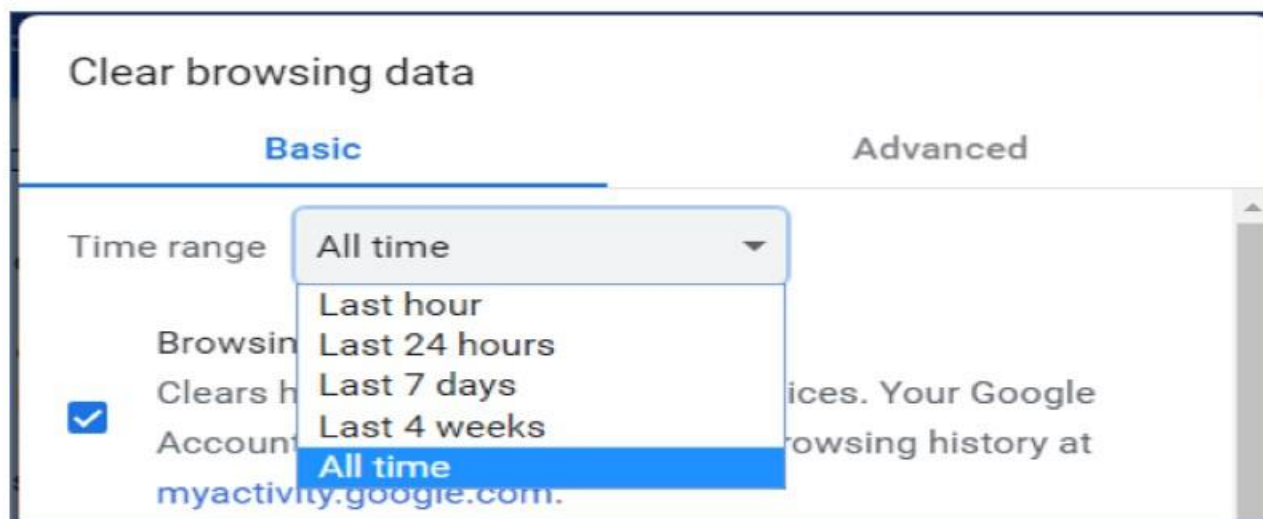
- Scroll down and click to the **Clear browsing data** option. The **Clear Browsing Data** window with different options such as browsing history, cookies and other site data, and cached images and files appears.





■ Google Chrome...

- Select the checkbox against the **Cached images and files** option.
- Click the **All time** dropdown arrow to display time range options. The dropdown time options appear as shown below.





- The effective password management is very fundamental in maintaining high level of security for online browsing and shopping.
- The frequent change of the passwords is one of the important components of effective password management.
- You should always choose the strongest password that has at least 14 characters that should also include:
 - Capital and lower-case alphabetic letters
 - Numeric characters
 - Special symbols





- The hackers continuously strive to break the operating system security by exploiting the vulnerabilities
- For making your online shopping and internet browsing experience safe, secure, and free of worries, always **keep your operating system up to date** by downloading and installing the latest updates released by the concerned teams of operating systems.





Many applications are designed to search for the updates automatically and prompt the user about that update to download. But in many cases, the third-party applications don't update automatically on the computers.

The examples of computer applications include:

- Google Browser (Google Chrome)
- Microsoft Skype
- Email Application
- Adobe Acrobat
- Java Applications
- Adobe Flash
- And many others





There are certain useful tips and guidelines for safe browsing and online shopping, which are listed below:

- Always use your personal data carefully and professionally
- Avoid to click unsolicited links and promotions
- Never use public networks for shopping purposes
- Always use secure connection with firewall enabled
- Always keep your privacy settings open/active
- Think twice before you download any software
- Avoid freebies and tempting offers
- Always use strong passwords
- Change your passwords within 60 or 90 days
- Always visit the secure websites that use https protocol
- Always shop from the trusted websites
- Keep your OS and applications up to date
- Clear your browser cache and browsing history regularly
- Keep antivirus and anti-spyware up to date
- Check you online shopping and bank statements regularly





- Don't follow the links in the phishing emails
- Try to use blurring software tools that blur your personal information while shopping
- Mobile apps for trusted merchants are better for shopping as compared to the online shopping through browser
- Try to use digital wallets rather than the credit or debit cards
- Try to pay through gift vouchers and other such prepaid cards for shopping
- Check the credibility of the merchant
- Send complaints immediately, if you find any suspicious activity on your account
- Read delivery and return policy of the merchant carefully
- Read privacy statements carefully
- Maintain a record of your online purchases
- Last but not the least, use your common sense always!





Cybersecurity Standards

Introduction

ISO/IEC27001
&27002 Standards

Information
Security Forum ISF
Standards

Payment Card
Industry Data Security
Standard PCI/DSS



Cyber Security Standards



- **Industrial standards** play a very critical role in all types of industries. **The standards are the defined guidelines, best practices and rules to achieve any certain objective in that particular industry.**
- In this chapter, we will talk about a few important standards that deal with the cyber security in the field of information and communication technology commonly referred to as ICT.
- There are many standard organizations, industry alliances and government authorities that devise different types of standards for different activities related to information and communication technology.
- The **standard organizations** develop standard through deep research with the help of the industry experts in the field of information technology. They develop certain formulas and criteria for different things, activities and procedures.



Cyber Security Standards



A few formulas and criteria for different procedures and activities are listed below.

- Security of the code of the web environment
- Criteria for the testing of the computer code
- Assessment of the vulnerabilities in the web environments
- Possible impact of the vulnerabilities on the industries and the end-users
- Ways to avert any kinds of security threat
- The assessment of the level of risk
- Assessing and implementing secure communication
- How to deal with the potential threats
- What preemptive measures can help avert any possible cyber threats
- And much more



Cyber Security Standards



In the nutshell, **the cyber security standards identify the most suitable ways and industry best practices that are implemented to establish an effective cyber security.** The detailed documents of the guidelines are also created; those documents establish the relationship between other security standards and guidelines. A detailed scope of work, roles, implementation procedure and audit process are created for smooth adoption of the standards in the organizations.

This is an international standard offered by ISO. It is also accepted all over the world. The organizations from any part of the world can adopt this standard for establishing information security control.

Let's discuss a few very important cyber-security standards that are commonly adopted in the field of information and communication technology.

- **ISO/IEC 27001 & 27002 Standards**
- **Information Security Forum ISF Standards**
- **Payment Card Industry Data Security Standard (PCI/DSS)**



These two standards deal with the information technology control within the IT organizations. This standard is developed by the International Organization of Standards commonly referred to as **ISO**. These standards are also written as ISO 2700X, which denotes both the cyber security standards as mentioned above.

- **The objectives of this standard include:**
 - Establishing information security controls
 - Reduce the security risk in the organization
 - Streamline the cyber security procedures
 - Selection of the information security controls
 - Management of information security controls
 - Implementation and monitoring of the information security controls



These standards allow the company to take the following steps:

- Choose the right controls over the information security processes for the organizations that are defined in the recommendations
- Implement the already accepted controls that have already been used and proven in different industries for IT controls
- Develop new information security controls that are in compliance with the set criteria in the ISO standards and also suit the requirements of the organization



These standards are constantly revised in the changed environment of the security threat and security risk profiles. So, always have a look at the revised versions of the standards.

ISO also provides certificates to the organizations that fully adopt these standards and implement them in accordance with the set criteria. The organization also audits the implementation of the standards on a regular basis. ISO certification requires charges even to access the detailed requirements.

There are four modules based on fixed prices, which will allow the IT organizations to achieve the certification of the ISO information security control standards. ISO has also a wide range of their consultant companies that work all over the world and deal with the organizations that are interested in the implementation of information security control standards.



Information Security Forum ISF is an IT governance organization that devises good practices for the organizations to deal with the risks associated to the information technology security. **The main focus of this organization is to provide the industry with the risks of the existing as well as the emerging security threats.**

The major areas that the ISF good practices cover include the following:

- Risk associated with the Agile software development methodology
- Privacy of information and the intelligence about the emerging threats
- Security aspects of Industrial Control Systems (ICS)
- Assessing and establishing the co-relationship between the operational risk and the information risk



This is also an international set of good practice acceptable worldwide. **These standards help the organizations in:**

- Helping the leaders and teams exploit new areas for improving productivity and efficiency while maintaining high-level of security against information risks
- Preparing the organizations to preempt the potential threats to reduce the risk through agility and preparedness
- Identifying the ways to implement the security standards in efficient and effective manner

This set of good practice improves the efficiency, agility, and effectiveness of the security personnel and organization leaders by improving their alertness and innovative thinking. This is a business focused set of good practice.



The PCI/DSS standard is focused to the **personal information of the online shopper**. This standard is developed by the PCI Security Standard Council. **The standard was developed to safe guard the bank and card information of the card users** who use their cards for online shopping.

This standard directly impacts the millions of the people across world. Security Standard Council helps the financial institutes and merchants to implement the standard guidelines devised by the council so that the card information of the people can be safeguarded easily.



The council consists of the following financial organizations:

- American Express
- MasterCard Inc
- Visa Inc
- JCB International
- Discover Inc
- And others

The PCI council focuses on the following organizations to help them safeguard the personal and financial information of the card users.

- Point-of-sales (POS) manufacturers
- Financial software developers
- Financial hardware developers
- Merchants of all sizes
- Financial institutes/banks



The main function of the council through its IT card security standards is to implement the card information security by:

- Implementing security related technology, policy, and best practices to the existing and upcoming financial processes used at the merchant and financial institute ends
- Helping hardware and software vendors to implement the security features and capabilities in their products at the development level.

At present, almost all financial institutes, and merchants implement and follow the PCI/DSS guidelines and standards.



Thank You



Appendix الملحقات

HTTP Protocol Websites

▪ Installing Security Certificate on Windows ISS Server...

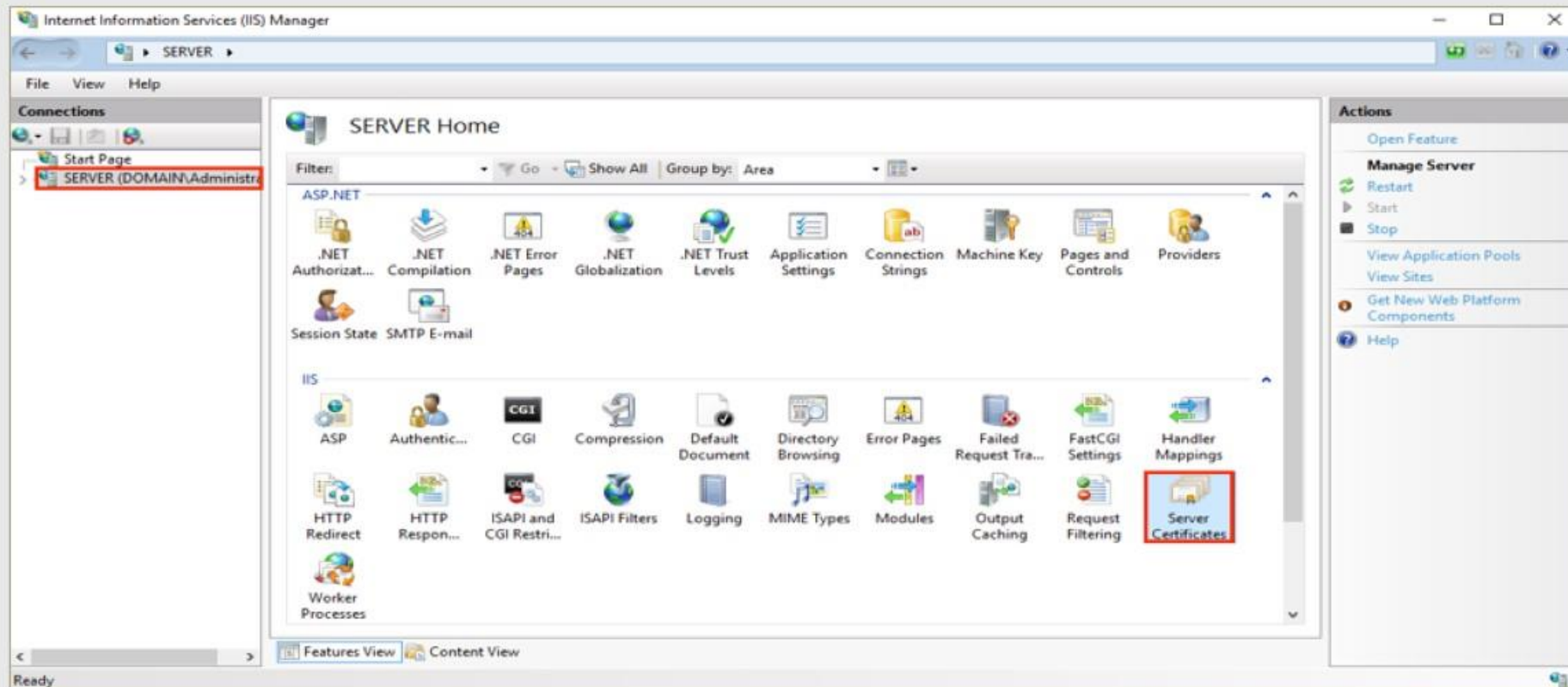
The latest version of **Windows Internet Information Service** (IIS) web server is v10. You need to purchase a digital security certificate commonly known as SSL certificate from the certificate authority and then install on your web server.

To install an SSL server on your website, take the following steps:

- Click **Start** menu, type **IIS Manager** in search bar, and open IIS manager. IIS Manager page appears
- In the left pane connection tree, locate and click the domain name of the web server. The **Server Home** window appears as shown in the following figure.

HTTP Protocol Websites

■ Installing Security Certificate on Windows ISS Server...



HTTP Protocol Websites

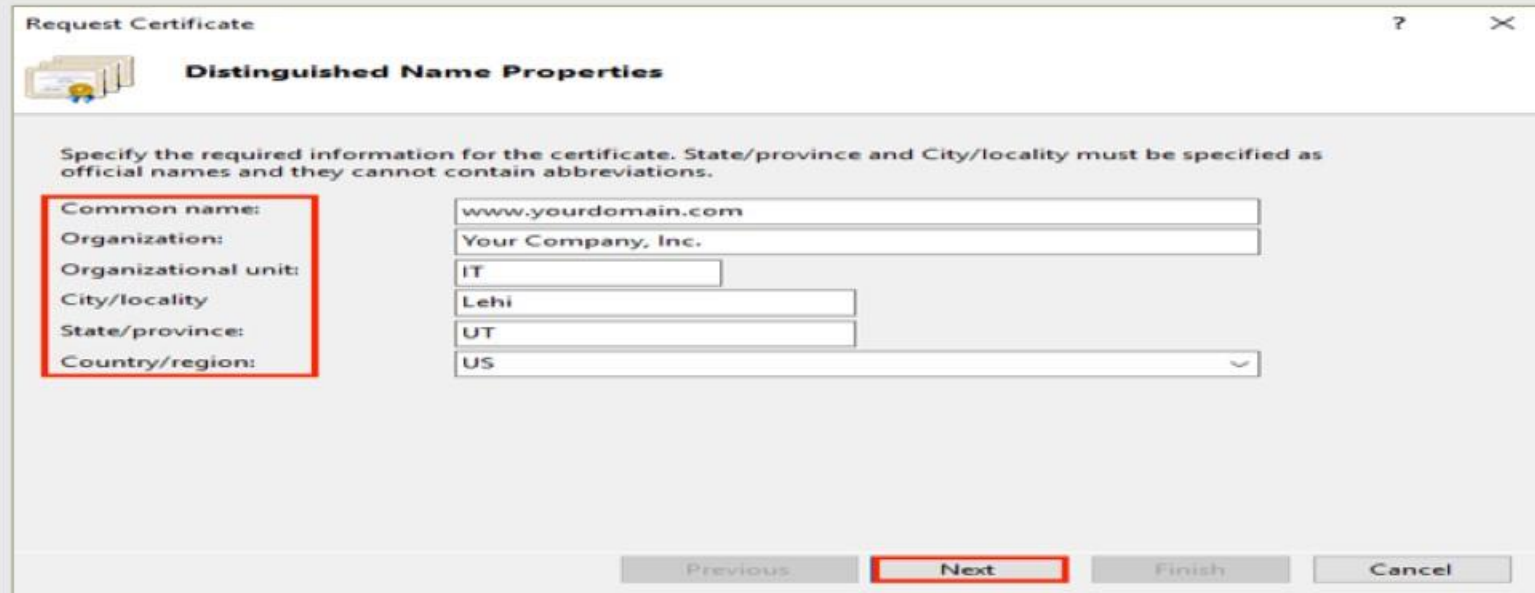
■ Installing Security Certificate on Windows ISS Server...

- Double click the **Server Certificates** icon. The server certificate page with existing list of certificates appears.
- On the right-pane, click the **Create Certificate Request...** link. The Request Certificate wizard with the distinguished name properties appears.
- Provide the detailed information about your website, company, organizations detailed physical address and other information required as shown in the following figure.

(Image on the next slide)

HTTP Protocol Websites

- Installing Security Certificate on Windows ISS Server...



The image shows a Windows dialog box titled "Request Certificate" with a subtitle "Distinguished Name Properties". It contains a list of fields on the left and corresponding input boxes on the right. The fields are: Common name, Organization, Organizational unit, City/locality, State/province, and Country/region. The input boxes contain the following values: www.yourdomain.com, Your Company, Inc., IT, Lehi, UT, and US. A red rectangle highlights the list of fields on the left. At the bottom, there are four buttons: Previous, Next, Finish, and Cancel. The "Next" button is highlighted with a red rectangle.

Request Certificate

Distinguished Name Properties

Specify the required information for the certificate. State/province and City/locality must be specified as official names and they cannot contain abbreviations.

Common name:	www.yourdomain.com
Organization:	Your Company, Inc.
Organizational unit:	IT
City/locality	Lehi
State/province:	UT
Country/region:	US

Previous Next Finish Cancel

- Click the **Next** button, when the required fields are filled with the valid information. The **Cryptographic Service Provider Properties** page appears.

HTTP Protocol Websites

- **Installing Security Certificate on Windows ISS Server...**

- Fill-up the name of the cryptographic service provider and the required SSL security bit length in the respective fields as shown below.

Request Certificate

Cryptographic Service Provider Properties

Select a cryptographic service provider and a bit length. The bit length of the encryption key determines the certificate's encryption strength. The greater the bit length, the stronger the security. However, a greater bit length may decrease performance.

Cryptographic service provider:
Microsoft RSA SChannel Cryptographic Provider

Bit length:
2048

Previous **Next** Finish Cancel

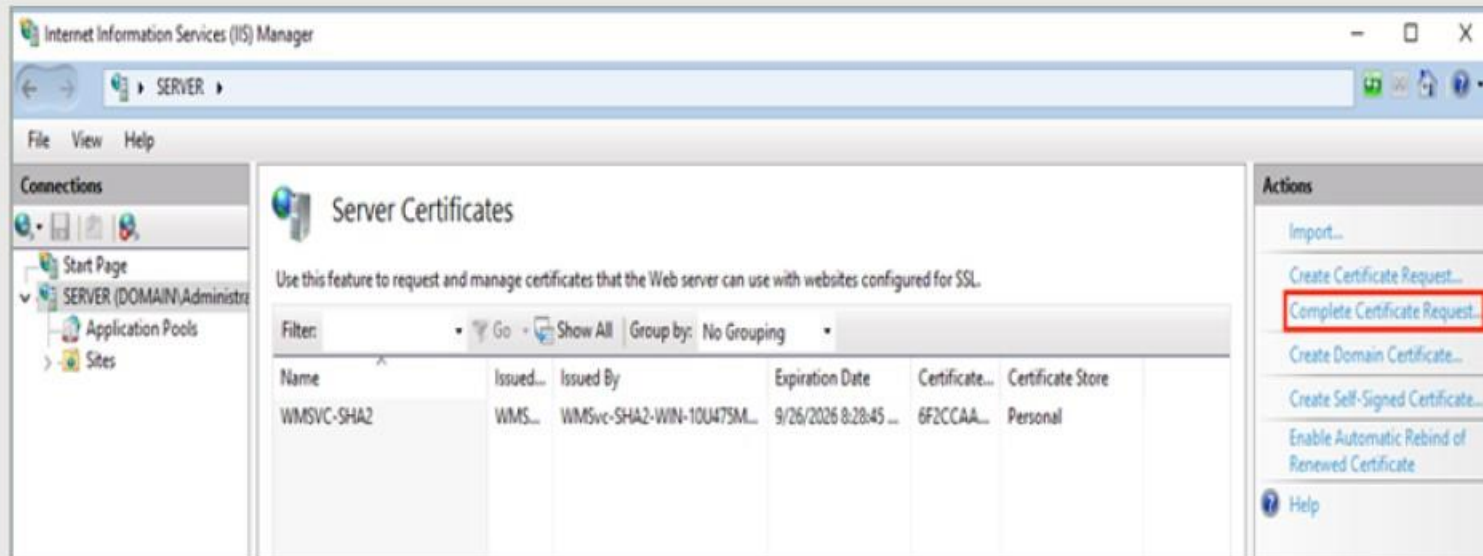
HTTP Protocol Websites

■ Installing Security Certificate on Windows ISS Server...

- Click the **Next** button. The **File Name** page appears.
- Choose the file name and location where you want to save that CSR file
- Click the **Finish** button. The CSR file will be created at the desired location.
- Open the CSR file and copy the entire text file and use the copied text to place order to the certificate authority (CA) website
- After some verifications, the CA will send you SSL Security Certificate through email
- Save the SSL Security Certificate on your computer
- Go to the **Server Certificates** page again.

HTTP Protocol Websites

- **Installing Security Certificate on Windows ISS Server...**



- Click the **Complete Certificate Request...** link in the right-page (**Action**), as shown in the above snapshot image. The **Specify Certificate Authority Response** page appears.

HTTP Protocol Websites

- **Installing Security Certificate on Windows ISS Server...**

- Enter the domain name of your website, select the hosting provider's name, and locate the certificate file response received from the certificate authority (CA) as shown in the following figure.

Complete Certificate Request

Specify Certificate Authority Response

Complete a previously created certificate request by retrieving the file that contains the certificate authority's response.

File name containing the certification authority's response:
C:\Users\Administrator\Desktop\certs\your_domain_name.cer

Friendly name:
yourdomain.com

Select a certificate store for the new certificate:
Web Hosting

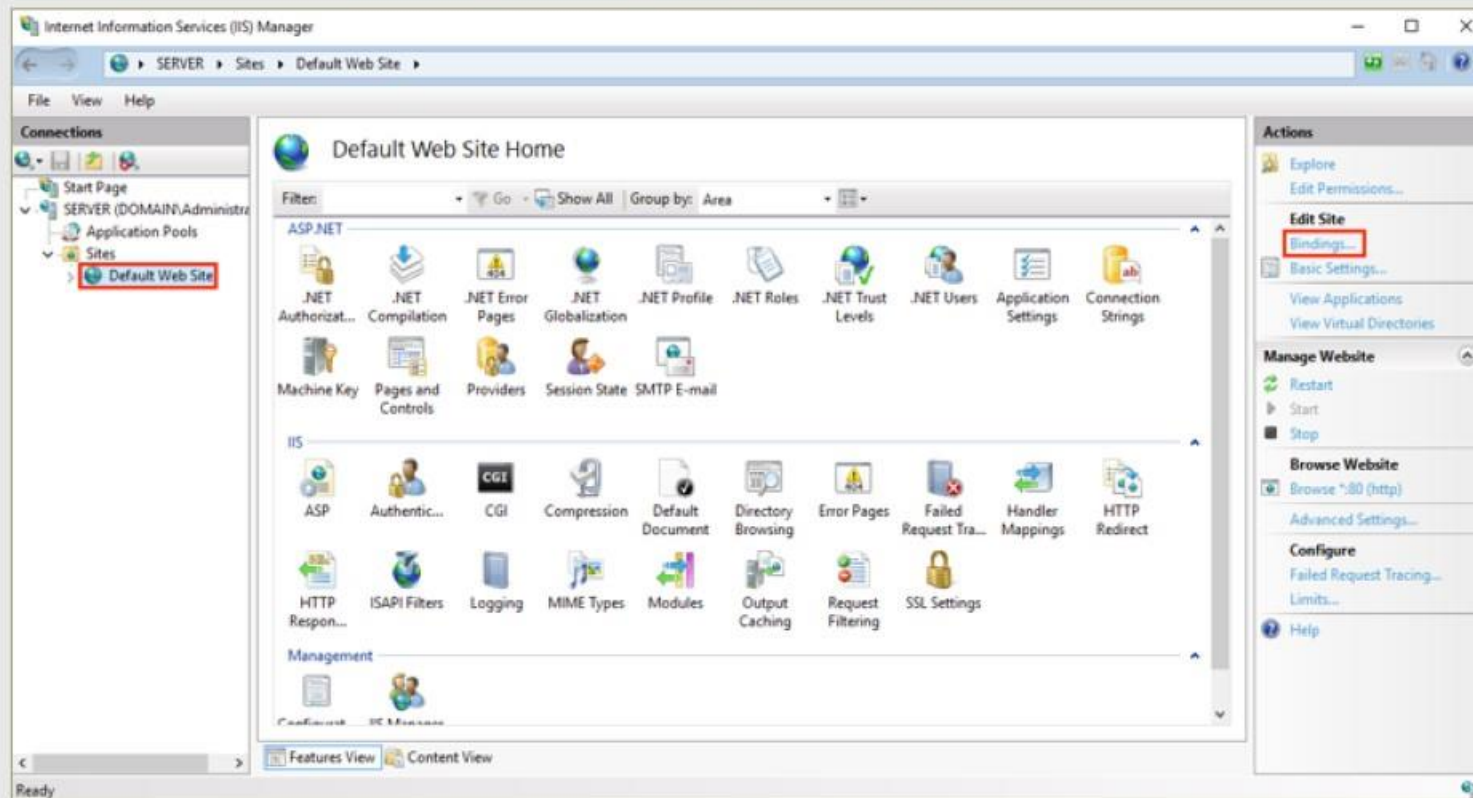
OK Cancel

HTTP Protocol Websites

- **Installing Security Certificate on Windows ISS Server...**
 - Click the OK button, once you are done with entering the required information. The SSL certificate is installed on your server successfully
 - Now, you need to assign the newly installed SSL to the desired website
 - On the **Internet Information Service IIS Manager** page, expand the **Server (Domain) Administration** page to locate the **Sites** option.
 - Click the **Sites** link in the left-page. The list of the existing websites appears
 - Click the desired website. In our example, it is **Default Web Site** option. The home page of the desired website appears as shown in the following image.

HTTP Protocol Websites

■ Installing Security Certificate on Windows ISS Server...



HTTP Protocol Websites

■ Installing Security Certificate on Windows ISS Server...

- Click the **Bindings...** under **Edit Site** option in the right-pane (**Actions**). The **Site Bindings** window appears
- Click the **Add...** button. The **Add Site Binding** window appears as shown in the following snapshot.

The screenshot shows the 'Add Site Binding' dialog box with the following fields and values:

- Type:** https (dropdown menu)
- IP address:** All Unassigned (dropdown menu)
- Port:** 443 (text box)
- Host name:** (empty text box)
- ☐ **Require Server Name Indication**
- SSL certificate:** yourdomain.com (dropdown menu)
- Select...** button
- View...** button
- OK** button (highlighted with a red box)
- Cancel** button

HTTP Protocol Websites

- **Installing Security Certificate on Windows ISS Server...**

- Choose **HTTPS** in the type field, the **All Assigned** option in the IP address field, and **443** in the port field
- Select the domain name for which you want bind the SSL certificate in **SSL Certificate** field.
- Click the OK button, when done with the data entry. Your website has been bound with the SSL certificate and you are ready to go.

You can also install multiple SSL certificates on your server and bind them with the multiple domain names of the websites by repeating the same step by step process as mentioned above.