Global Information Assurance Certification Paper

What is Secure Outlook Web Access (SSL-OWA)?
Cliff Rittel
September 13, 2000

What is OWA?

Microsoft OWA for Exchange Server offers the ability to access secure e-mail, calendar, scheduling and collaboration applications using the Internet Explorer Web Browser. A server running Exchange 5.5 and Internet Information Server are required on the backend. The IIS server uses active server pages to handle the requests and interact with the central log on server for authenticity and the Exchange Information Store for access to a mailbox. Mailbox information can only be accessed while client/server on-line connectivity exists. This application is used primarily as a central server application service, which remote clients connect to over the public Internet. Due to the inherent insecurity of the Internet, security settings such as SSL need to be put in place.

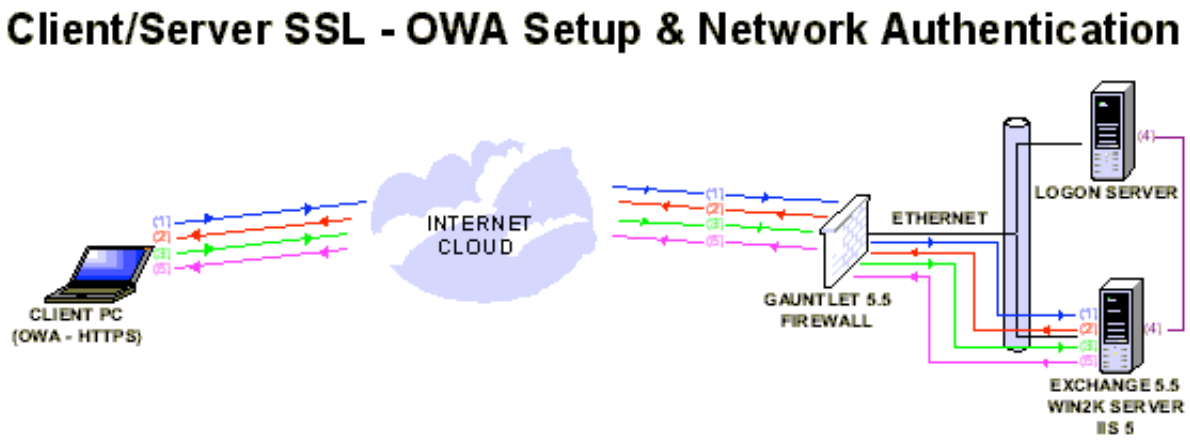
What is ASP and SSL?

ASP is an acronym for Application Server Provider and refers to an environment where clients access a central server over the Internet, and the core data resides on the server. The OWA connection fits the ASP model because all of the data is centrally hosted and decentralized clients are accessing the data. Typically, ASP

SSL is an acronym for Secure Sockets Layer which is a protocol developed by Netscape Communications to provide secure data transmissions over the Internet. SSL is a transport layer security technique that can be applied to HTTP and provide privacy between two communicating devices, as this paper will demonstrate the Windows client and the Exchange/IIS server. SSL provides mandatory authentication, encryption and data integrity. The protocol mandates data transmissions by a session key so that data transmissions cannot be altered or disclosed. A more in depth understanding of the SSL transaction will be established in the next sections.

Setup of OWA

For my test, I used Windows clients (98/NT/2000) connected to dial up, cable modem and T1 connections over the Internet to illustrate the ASP functionality. Please note IE is required as OWA connectivity will not work with Netscape or any other Internet Browser. I used NAI's Gauntlet 5.5 firewall and built a proxy to handle the connection. On the LAN, I used a standard Intel server configuration running Windows2000 SP1, Exchange 5.5 SP3 and IIS 5. For SSL I used a server certificate issued by a publicly trusted root CA, Thawte, and installed it on the IIS server. I only required server side authentication, but to add an additional layer of authentication security one could require the client have a valid SSL certificate (see IIS SSL ENABLE SETUP). Below is a diagram of the network topology, screen shots of the log on transaction and further explanation of the SSL/OWA and network authentication transaction.



SSL Transaction

In order for the SSL transaction to work both the client (IE) and the Server (IIS) must be SSL enabled. The transaction runs over TCP. (1) The security transaction begins when the client sends a request to the server for its digital certificate. Traditionally, this begins with typing https: in the URL locator. (2) The server sends its digital

certificate to the client. The client will check the digital certificate for accuracy in terms of issuance from a trusted root Certificate Authority, valid date on the certificate and common name of the certificate. If there are any problems the user has the option to view the certificate, continue or cancel the transaction. (3) If the client continues, then the client authenticates the server by decrypting the digital signature that is within the digital certificate. The client then generates a session key and encrypts it using the server's public key from the certificate sends it to the server. Once the server receives the session key it uses it to encrypt and decrypt the data tunnel. SSL uses message authentication to ensure tampering with data transferred between the client and server has not taken place.

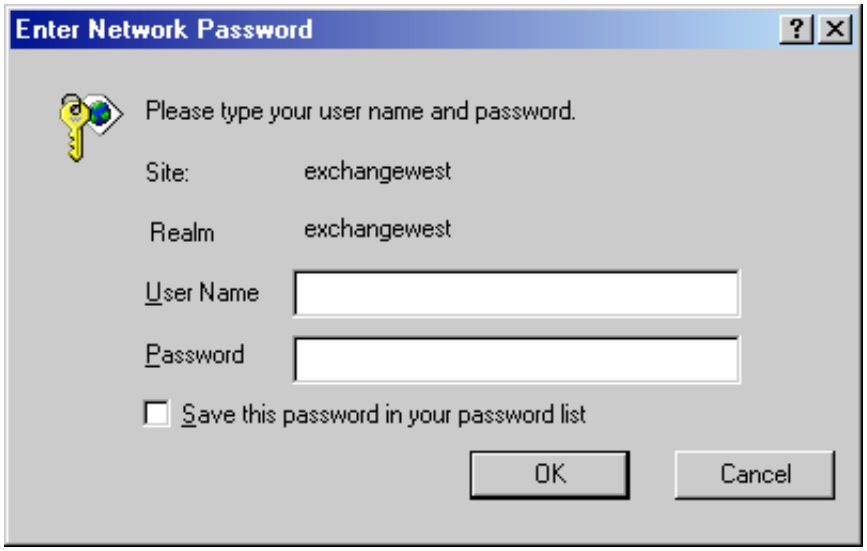
Example (2)

Logon Authentication

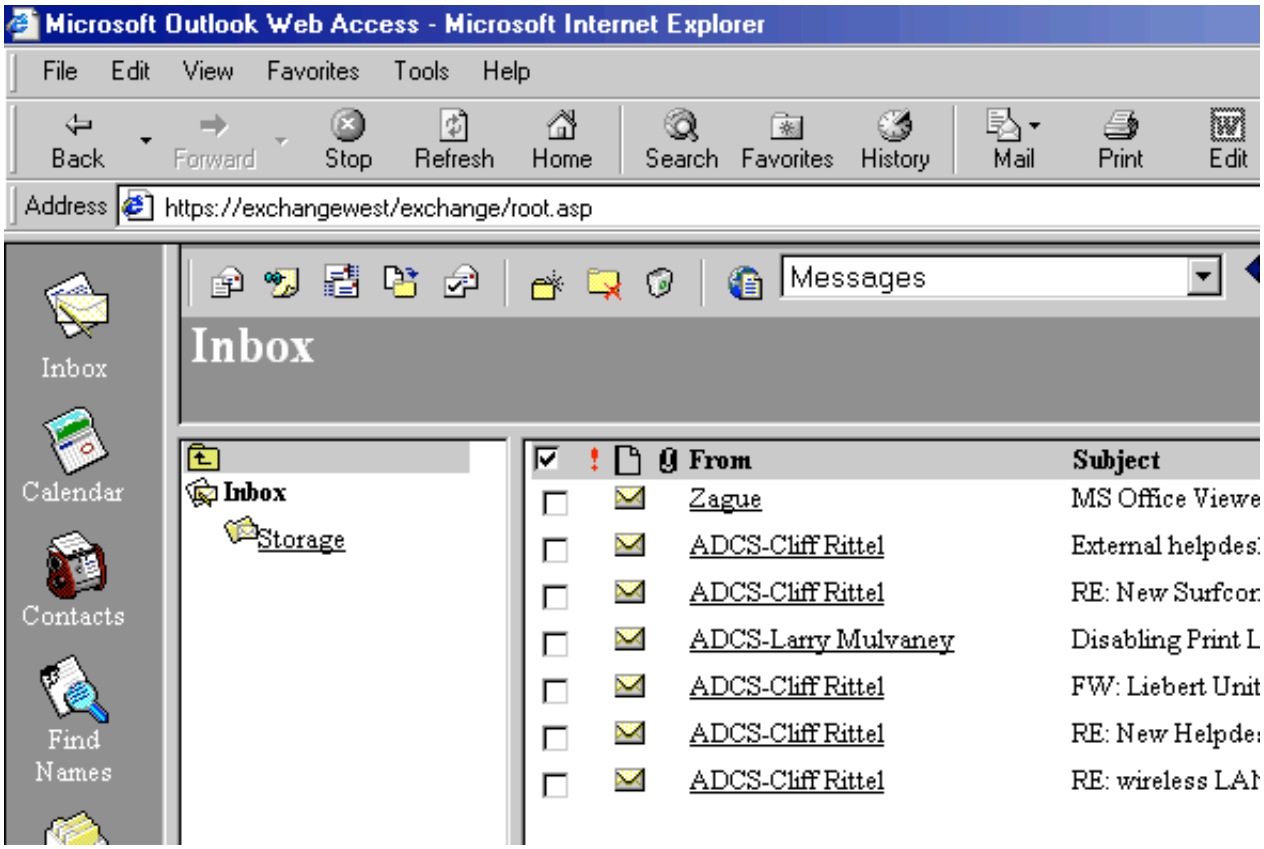
Once the SSL session is established between the client and server, the server requests from the client a user alias mailbox on the client. (4) Then the client is prompted for its network logon credentials, which it then authenticates with a Logon Server. (5) Once authenticated with a valid user account the Exchange server offers the client access to their mailbox resources.

OWA Log On Mailbox Alias Screen

Network Logon Server Screen (4)



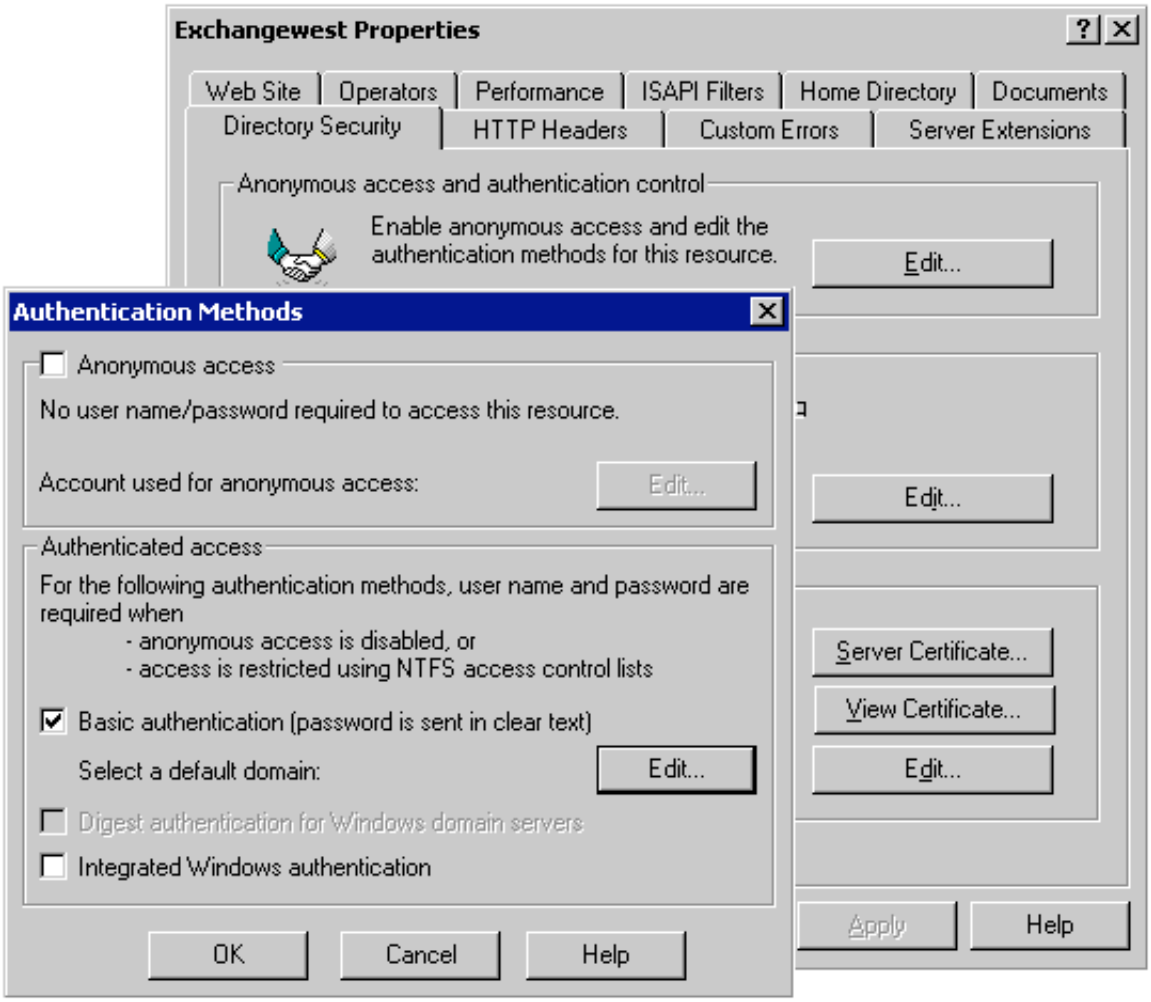
Mailbox Resource Screen (5)



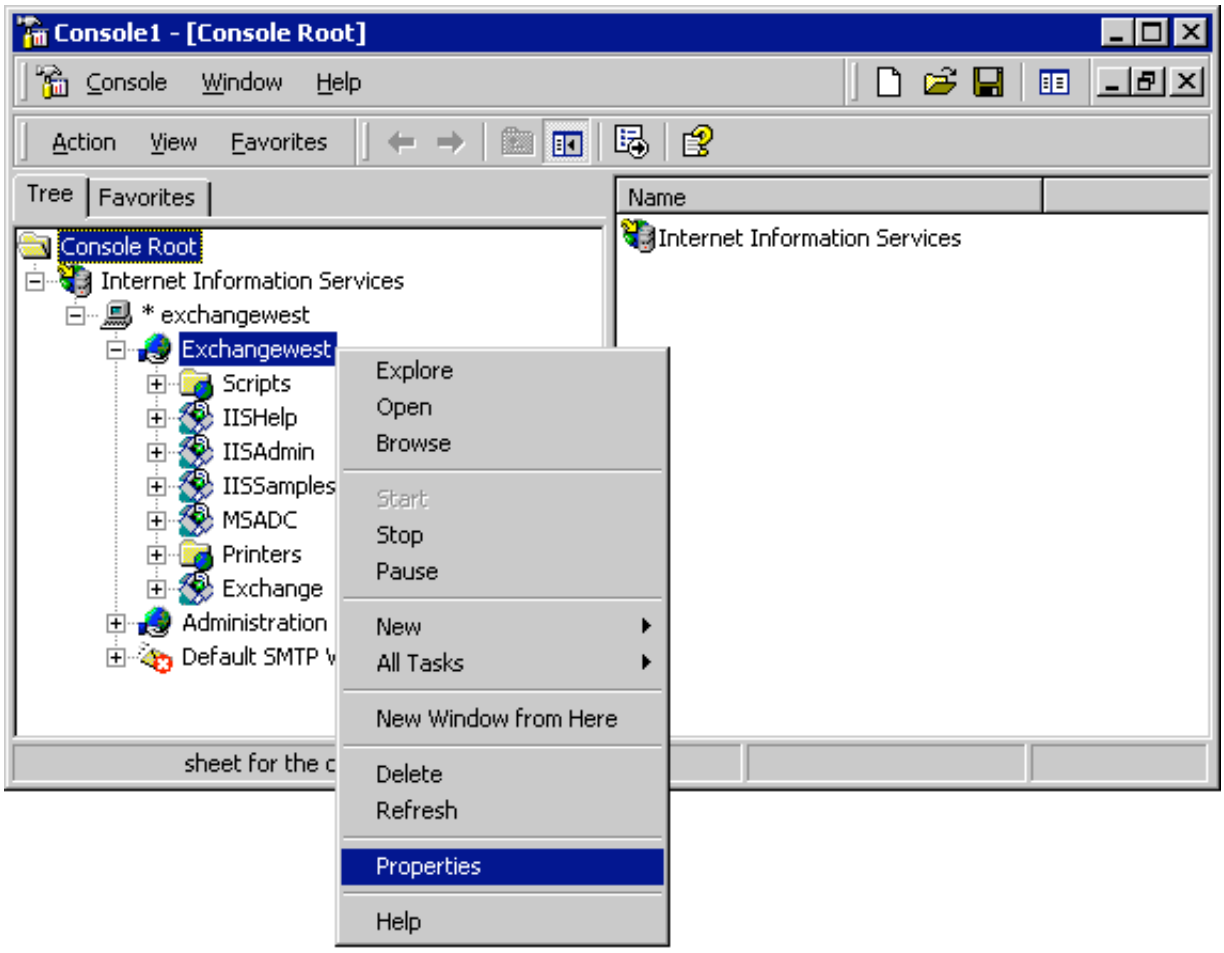
IIS SSL Enable Setup

As noted previously, the test installation was on a Windows2000 SP1 platform with Exchange Server 5.5 SP3 and Internet Information Server 5. The following screen shots give a graphical presentation on how to set up SSL within IIS. The SSL connection has additional security options such as requiring the browser to establish 128 bit encryption or mandating client certificates.

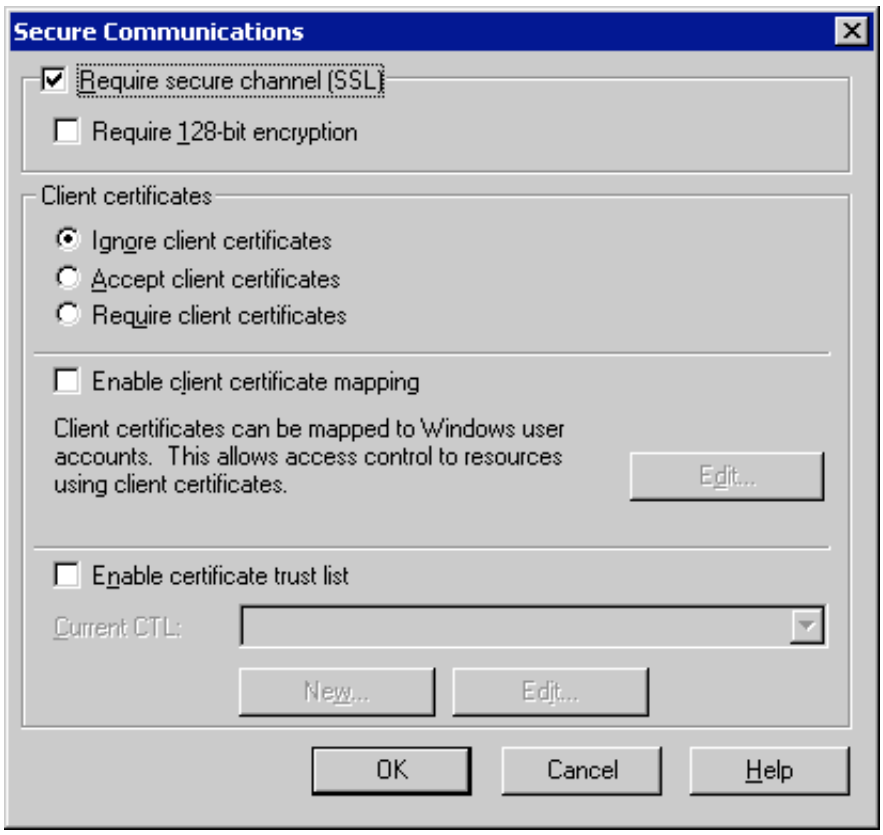
Properties of IIS Web Server



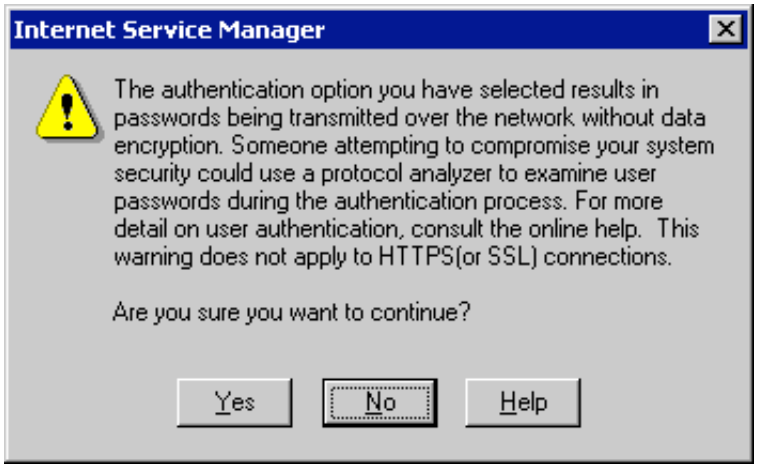
Manage Secure Communications



Very important security warning message



This screen shows SSL connection options.



Conclusion

OWA over a SSL connection can offer an effective, secure communication over the public Internet to an Exchange mailbox. OWA operates as an ASP host, which increases the ability to tighten security in a central location. OWA installations without SSL are a security risk as users will send their passwords in clear text over the Internet. SSL ensures authentication, encryption and data integrity. When establishing any type of remote access into an internal network a well thought out plan is essential to ensure the highest level of security possible in protecting precious Information Systems.

References

Microsoft Corporation. (1999). "Planning and Deploying Outlook Web Access 5.5". Microsoft Corporation. Redmond, WA. White Paper.

Microsoft Corporation (1999). "ASP Certification White Paper". Microsoft Corporation. Redmond, WA. http://www.microsoft.com/ISN/downloads/ASP%20Certification%20White%20Paper.doc White Paper.

Minoli, Daniel, E. Minoli. (1998). Web Commerce Technology Handbook. McGraw-Hill Companies Inc. New York, NY.

Network Associates Technology, Inc. (1996-1999). Gauntlet Firewall/VPN for WindowsNT Getting Started Guide v5.5. Network Associates Technology, Inc. Santa Clara, CA.

Thawte - A Verisign Company. www.thawte.com

Last Updated: July 20th, 2017

Upcoming Training

SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
Community SANS Trenton SEC401	Trenton, NJ	Aug 21, 2017 - Aug 26, 2017	Community SANS
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event