SecurEnvoy
A Shearwater Group plc Company

www.securenvoy.com

SecurAccess Security Guide

SecurAccess IIS Security Hardening Guide

Version 1.0 – 02/19

SecurAccess Security Guide

Contents

1.1 Solution Summary

SecurEnvoy's SecurAccess MFA solution provides user self-service portals to aid in the user enrolment, password change, helpdesk and administration purposes.
All SecurAccess portals are hosted through Microsoft's IIS web server platform and will present all portals unless IIS is locked down to the business requirements.

The software used for this guide is listed below:

SecurEnvoy SecurAccess Release v9.3.502
Windows Server 2016 (IIS – Version 10.0.14393.0)

1.2 Guide Usage

The information in this guide describes the configuration steps required to implement a more secure (hardened) SecurAccess and Microsoft IIS (Internet Information Services) platform.
The hardening information provided is intended primarily for Microsoft administrators, and for the technical operator of each component that is involved in the implementation of a secure SecurAccess solution (for example, the Web Server). These people should familiarize themselves with the hardening settings and recommendations prior to beginning the hardening procedures.

NOTE:
In this document, the term reverse proxy also refers to load balancing in Layer 7 or WAF (Windows Application Firewall)

1.3 Deploying SecurAccess in a Secure Architecture

Several measures are recommended to securely deploy your SecurAccess Server.

Reverse proxy architecture

One of the more secure and recommended solutions is to deploy SecurAccess using a reverse proxy.

SecurAccess fully supports reverse proxy architecture as well as secure (SSL Offload) reverse proxy architecture.

The following security objectives can be achieved by using a reverse proxy in a DMZ proxy HTTP/HTTPS communication method.

- No direct communication between public facing clients and SecurAccess servers.
- No direct connection from the DMZ to the APM database is required.
- The protocol used to communicate with the reverse proxy is typically HTTPS, Offloaded before the SecurAccess server and inspected unencrypted at the firewall level if required.
- Most of the Web server security features are available on the reverse proxy (authentication methods, encryption, URL/Content restriction and others).
- The reverse proxy screens the IP addresses of the real SecurEnvoy servers as well as the architecture of the internal network.
- The only accessible client of the SecurAccess server is the reverse proxy.
- Configuration supports NAT firewalls.
- Reverse proxy requires minimal number of open ports in the firewall

1.4 Notes and Recommendations

To best use the hardening guidelines given here for your particular organization, do the following before starting the hardening procedures:

- Evaluate the security risk/security state for your general network, and use the conclusions when deciding how to best integrate the SecurAccess platform into your network
- The hardening procedures are based on the assumption that you are implementing only the instructions provided in this guide, and not performing other hardening steps not documented here.
- Where the hardening procedures focus on a particular distributed architecture, this does not imply that this is the best architecture to fit your organization's needs.
- It is assumed that the procedures included in the hardening guide will be performed on machines dedicated to the SecurAccess platform. Using the machines for other purposes in addition to SecurAccess may yield problematic results.

1.5 General Security

HTTP Strict Transport Security (HSTS) is a web security policy tool that helps to protect websites against protocol downgrade attacks, cookie hijacking, and variants of man-in-the-middle attacks. It enables web servers to enforce that web browsers (or other complying user agents) should only interact with secure HTTPS connections, and not through the insecure HTTP protocol. For more information about HSTS, see RFC 6797.

HSTS provides two methods for sites to secure their connections:

Registering for a preload list: You can register your websites to be hardcoded by major browsers to redirect HTTP traffic to HTTPS. This ensures that communications with these websites from the initial connection are automatically upgraded to be secure. The preload list is based on the Chromium HSTS preload list. From more information, see https://www.chromium.org/hsts.

Enabling HSTS on your server: For sites not on the preload list, you can enable HSTS via the Strict-Transport-Security HTTP header. After an initial HTTPS connection from the client containing the HSTS header, the browser redirects all subsequent HTTP connections to be secured via HTTPS.
For IIS 7.0 and higher:

1. Open a cmd window with administrative privileges and run the following command:

%SystemRoot%\System32\inetsrv\appcmd set config /section:httpProtocol /+customHeaders.[name='Strict-Transport-Security',value='max-age=31536000']

2. Restart IIS by running the iisreset command in the same cmd session.

1.6 Strong Cipher Suite Order

To protect against attacks on 64-bit block ciphers in TLS, you need to configure a strong cipher suite order.

1. In Microsoft IIS, you can use the following methods to configure a strong cipher suite order:

Using GPO:

a. At a command prompt, run gpedit.msc to open the Group Policy Object Editor.

b. In the Local Computer Policy tree, expand Computer Configuration, Administrative Templates, Network, and then click SSL Configuration Settings.

c. In the right pane, click SSL Cipher Suite Order.

d. Click Policy setting and select enabled.

e. Set up a strong cipher suite order using Mozilla's TLS configuration instructions (see https://wiki.mozilla.org/Security/Server_Side_TLS) and the following list of Microsoft's supported ciphers:

TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,TLS_DHE_RSA_WITH_AES_128_GCM_SHA256,TLS_DHE_RSA_WITH_AES_256_GCM_SHA384,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,TLS_DHE_RSA_WITH_AES_128_CBC_SHA256,TLS_DHE_RSA_WITH_AES_128_CBC_SHA,TLS_DHE_RSA_WITH_AES_256_CBC_SHA256,TLS_DHE_RSA_WITH_AES_256_CBC_SHA,TLS_RSA_WITH_AES_128_GCM_SHA256,TLS_RSA_WITH_AES_256_GCM_SHA384,TLS_RSA_WITH_AES_128_CBC_SHA256,TLS_RSA_WITH_AES_256_CBC_SHA256,TLS_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_256_CBC_SHA,TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384,TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA,TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384,TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384,TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384,TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA,TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256,TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA,TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256,TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA,TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256

Using IISCrypto tool https://www.nartac.com/Products/IISCrypto enables you to set/change the appropriate Schannel settings using a simple and intuitive UI.

2. After creating the strong cipher suite order, restart IIS.

1.7 Issuing TLS Certificates

Secure communication via https can terminate either at the load balancer/ reverse proxy or on the SecurAccess server.
If it terminates on the SecurAccess server, the IIS web server on the server is configured to support/require TLS. Otherwise, if TLS terminates on the load balancer/reverse proxy, then only the load balancer/reverse proxy needs to be configured for secure communication.

Generally, server certificates must be issued to the name of the external portal (FQDN) that is configured in SecurAccess Server.
This is the name that users use to access the "Manage My Token" Portal e.g.
https://host.domain.com/secenrol

If there is a load balancer/reverse proxy in front of a SecurAccess server, it is recommended to have TLS terminate on the load balancer/reverse proxy.

TLS Termination On	TLS on Load Balancer	TLS on Server	Advantages/ Disadvantages
Load Balancer. Reverse Proxy or WAF	Yes	No	This is a recommended configuration. It allows: • Maintenance of certificates in one place (on load balancer/reverse proxy) • Reduced processing of load on APM Gateways On each load balancer/reverse proxy, use server certificates issued to the name of the external access point (FQDN) that users/data collectors are using to access SecurAccess. If multiple load balancers/reverse proxies share the load, each one must have these certificates imported.
Load Balancer and Server (TLS all the way)	Yes	Yes	This is a less ideal configuration, especially where load balancers are concerned. It requires: • Maintenance of certificates in multiple places (load balancer/reverse proxy and Server) • Expensive TLS renegotiation in load balanced environment for data collectors (see note below) In this configuration, in addition to installing certificates on the load balancer, also install certificates on the Server, using a certificate issued to the FQDN name of the server portals. In a high availability environment with multiple servers: very expensive in terms of CPU use and network traffic, on both the server and client sides. For this reason, TLS termination is typically done on the load balancer.
Gateway	No	Yes	Not a recommended scenario.

- Remember to remove HTTP from the Bindings of your server if you intend to use TLS on the server directly at not use a Load balancer, Reverse Proxy or WAF

1.8 Additional Security Recommendations

To provide additional security for access to the SecurEnvoy Server, we recommend the following:

Remove Server Header. By default, Microsoft adds a server response header with content looking like this `Server: Microsoft-IIS/7.5.`

It is recommended to remove this header.

1. Download and install URL Rewrite (if it is not already installed). See http://www.iis.net/downloads/microsoft/url-rewrite

2. Click Add Rule(s) and create a new blank outbound rule. Complete the following information:

- Name: Remove response server
- Matching scope: Server variable
- Variable name: RESPONSE_SERVER
- Variable value: Matches the Pattern
- Using: Regular Expressions
- Pattern: .+
- Action type: Rewrite
- Value: type bogus server name. For example, apache etc.
- Replace existing server variable value: Select this option.

3. Apply and use a header sniffer to check the results

X-Frame-Options header

Framesniffing is an attack technique that takes advantage of browser functionality to steal data from a website. Web applications that allow their content to be hosted in a cross-domain IFRAME may be vulnerable to this attack.

Administrators can mitigate framesniffing by configuring IIS to send an HTTP response header that prevents content from being hosted in a cross-domain IFRAME.

The X-Frame-Options header can be used to control whether a page can be placed in an IFRAME. Because the Framesniffing technique relies on being able to place the victim site in an IFRAME, a web application can protect itself by sending an appropriate X-Frame-Options header.

To configure IIS to add an X-Frame-Options header to all responses for a given site, follow these steps:

1 Open Internet Information Services (IIS) Manager.
2 In the Connections pane on the left side, expand the Sites folder and select the **default web site** you want to protect.
3 Double-click the HTTP Response Headers icon in the feature list in the middle.
4 In the Actions pane on the right side, click Add.
5 In the dialog box that appears, type **X-Frame-Options** in the Name field and type **SAMEORIGIN** in the Value field.
6 Click OK to save your changes.

X-XSS-Protection

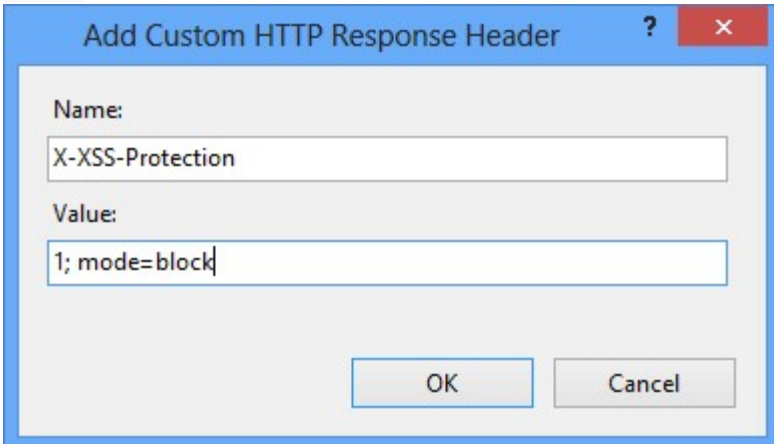
X-XSS-Protection header can prevent some level of XSS (cross-site-scripting) attacks, and this is compatible with IE 8+, Chrome, Opera, Safari & Android.

There are four possible ways you can configure this header.

Parameter Value	Meaning
0	XSS filter disabled
1	XSS filter enabled and sanitized the page if attack detected
1;mode=block	XSS filter enabled and prevented rendering the page if attack detected
1;report=URL	XSS filter enabled and reported the violation if attack detected

We will implement 1;mode=block in the default web server.

1 Open Internet Information Services (IIS) Manager.
2 In the Connections pane on the left side, expand the Sites folder and select the **default web site** you want to protect
3 Double-click the HTTP Response Headers icon in the feature list in the middle.
4 In the Actions pane on the right side, click Add.
5 In the dialog box that appears, **X-XSS-Protection** in the Name field and type **1;mode=block** in the value field and click Ok



6 Restart IIS

X-Content-Type-Options

1 Open Internet Information Services (IIS) Manager.

2 In the Connections pane on the left side, expand the Sites folder and select the **default web site** you want to protect

3 Double-click the HTTP Response Headers icon in the feature list in the middle.

4 In the Actions pane on the right side, click Add.

5 In the dialog box that appears, **X-Content-Type-Options** in the Name field and type **nosniff** in the value field and click Ok

7 Restart IIS

Disable unused portals

Following the installation of SecurAccess, a number of portals are installed within IIS by default. If a load balancer, reverse proxy or WAF is not being utilised to secure public facing access to SecurAccess portals, it is advisable to disable access to the additional portals through IIS if not removed through the program installer.

The following portals are installed into IIS following a TYPICAL installation of SecurAccess

IIS Site	Description of Use
password	Used to deliver self-service password reset (SecurPassword)
secadmin	Used to provided administrator access to the SecurAccess server (Highly recommended to only publish internally)
secconnector	Used to provide connectivity between on-premise connector agent and SecurEnvoy cloud
secenrol	Used for enrolment of user tokens, lifecycle management of tokens and PUSH notification through Mobile Authenticator
sechelp	Used for HTML help files of SecurAccess
sechelpdesk	Used for user self-serve token recovery and mobile number change (SMS Tokens)
secmail	Used for SecurMail
secmailsender	Used for SecurMail sending portal
secrep	Deprecated – Server Replication in multi-server deployment
secrest	Used by SecurAccess RESTful API
secserver	Used for SecurMail Outlook Agent communication
secupload	Used for SecurMail
secupload2	Used for SecurMail
securenvoy	Used as a User Portal URL Reminder/Bookmark

Please Reach Out to Your Local SecurEnvoy Team...

UK & IRELAND

The Square, Basing View
Basingstoke, Hampshire
RG21 4EB, UK

Sales

E sales@SecurEnvoy.com
T 44 (0) 845 2600011

Technical Support

E support@SecurEnvoy.com
T 44 (0) 845 2600012

EUROPE

Freibadstraße 30,
81543 München,
Germany

General Information

E info@SecurEnvoy.com
T +49 89 70074522

ASIA-PAC

Level 40 100 Miller Street
North Sydney
NSW 2060

Sales

E info@SecurEnvoy.com
T +612 9911 7778

USA - West Coast

Mission Valley Business Center
8880 Rio San Diego Drive
8th Floor San Diego CA 92108

General Information

E info@SecurEnvoy.com
T (866)777-6211

USA - Mid West

3333 Warrenville Rd
Suite #200
Lisle, IL 60532

General Information

E info@SecurEnvoy.com
T (866)777-6211

USA – East Coast

373 Park Ave South
New York,
NY 10016

General Information

E info@SecurEnvoy.com
T (866)777-6211

SecurEnvoy
A Shearwater Group plc Company

www.securenvoy.com