

Sniffa Runbook Adding the Web Portal Application to Internet Information Services (IIS)

Serial	Instruction	
	Overview The Sniffa Sensor Manager Web Portal Application is an intuitive graphical user interface for analysing network traffic metadata and viewing Snort [™] and/or Zeek [™] Alerts. The Web Portal is designed to allow users controlled access to the data stored in the Sensor Manager Application Database. The Web Portal Application is an ASP.NET application, developed to be installed and run on a Microsoft [™] Windows Internet Information Services (IIS) Server. This runbook includes the tasks to be completed, to add the Web Portal Application to an IIS Server running on a Microsoft [™] Windows host.	
1.	Add Windows™ IIS to your version of Windows.	Internet Information Services (IIS) Manager
2.	Open Windows™ Explorer and go to 'Control Panel\Programs\Programs and Features'. Select 'Turn Window features on or off'.	 Programs and Features ← → ✓ ↑
3.	Check 'Internet Information Services. Check 'Web Management Tools'. Check 'World Wide Web Services'. Check 'Application Development Features'. Check 'ASP.NET 4.8' or above. Click on the button marked 'OK' to save.	Windows Features - × Turn Windows features on or off Image: Comparison of the feature off, clear its checkbox. A filled box means that only part of the feature is turned on. Internet Explorer 11 Image: Internet Information Services Image: Internet Information Services Image: Internet Information Services Image: Internet Information Services Image: Internet Information Service Image: Internet Information Service Image: I





Sniffa Runbook Adding the Web Portal Application to Internet Information Services (IIS)

4.	Start IIS from the Windows™ Start Icon.	Age Decements Web More • Image: Image
5.	Right click on the 'Site' tree menu item and click on 'Add Website'.	Internet Information Services (IIS) Manager Image: Strain Services (IIS)
6.	Add Site name. Add Physical path. <i>Note:</i> <i>Default physical path is shown</i> . Set up Binding (http or https) and Port. Add Certificate. Click on the button marked 'OK' to save.	Add Website ? × Site name: Application pool: newsite newsite Content Directory Physical path: Corporam Files (x86)/SniffaServer/portal Pass-through authentication Connect as Test Settings Binding Type: IP address: Port: https All Unassigned Host name: Disable TLS 1.3 over TCP Disable QUIC Disable TLS 1.3 over TCP Disable HTTP/2 Disable OCSP Stapling Start Website immediately



Sniffa Runbook Adding the Web Portal Application to Internet Information Services (IIS)

7.	Select the new site. Ensure that the ASP.NET icons are showing.	newsite Home reter: - *** - *** - ***
8.	Select 'Connection Strings'.	Connection I Strings
9.	<pre>Add a Connection String that matches the environment. Using a MS SQL Server: Server=localhost\; Database=sniffa; User Id=sniffaadmin; Password=*********; Using a MS SQL Server Express: Server=localhost\SQLEXPRESS; Database=sniffa; User Id=sniffaadmin; Password=********; Using the MS SQL Server Express LocalDB: Data Source=(localdb)\v11.0; AttachDbFileName=C:\Program Files (x86)\SniffaServer\sniffa.mdf; Initial Catalog=sniffa; Note: input correct password instead of **********</pre>	
10.	Open a Browser Application and go to https://localhost:[port number] Login with a valid username and password. Note: Replace [port number] with the correct port number if not the default 443 for https or 80 for http.	e Use Account Details to Sign In waraaraaraa managra managra maanagra contails
11.	If the Connection String is incorrect, an error screen will be shown when the button marked 'Sign In' is clicked. Correct the Connection String and try again.	Copy: Scorething that goes array





12.	Firewall Settings. Open Windows Defender Firewall from the Windows Start Menu. Click on the Menu Item marked 'Advance settings' from the left hand menu.	Windows Defender Firewall Control panel
13.	Select 'Inbound Rules' from the left hand menu. Select 'New Rule' from the right hand menu.	Windows Defender Firewall witl Windows Defender Firewall witl Outbound Rules Actions Inbound Rules New Rule
14.	Add a new rule to allow port TCP 443. <i>Note:</i> <i>Replace [port number] with the correct</i> <i>port number if not the default 443 for</i> <i>https or 80 for http.</i> Give the rule a unique name and click the button marked 'Finish' to save and enable the rule.	Mew Inbound Rule Wizard × Protocol and Ports Seedy the protocols and ports to which this rule apples. Seedy the protocols and ports to which this rule apply to TCP or UDP? Protocol and Ports Oces this rule apply to TCP or UDP? Profie Name Dees this rule apply to al local ports or specific local ports? All local ports @ Specific local ports: 443 Example: 80, 443, 5000-5010
15.	End of Runbook.	