User Guide for the Oracle Service Cloud TLS 1.0 Log Scanner

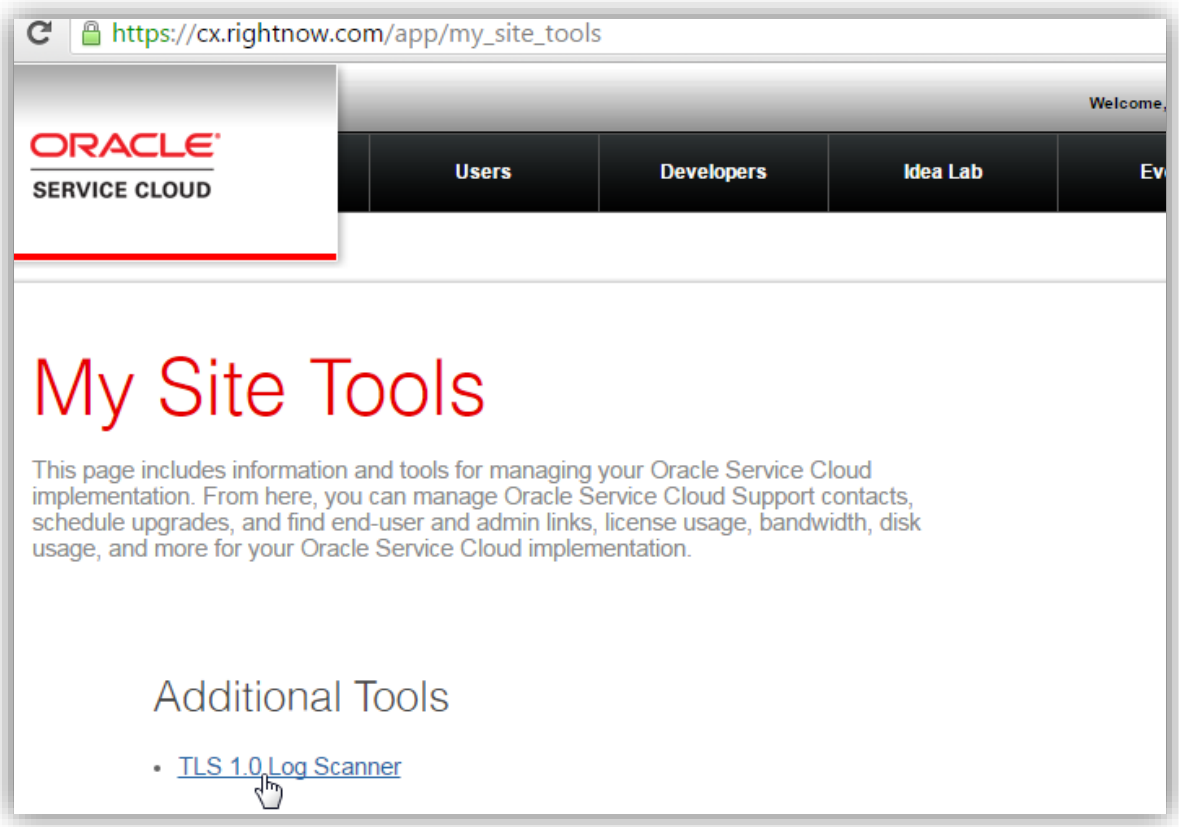
Introduction

In order for Oracle Service Cloud customers to readily identify TLS 1.0 usage, Oracle created the TLS 1.0 Log Scanner. The TLS 1.0 protocol is being abandoned, so you must remediate any current use of it. On a weekly basis, the Log Scanner readily identifies for you where TLS 1.0 is being used within your Oracle Service Cloud instance(s). This simple user guide explains how to access and use the Log Scanner.

Accessing the TLS 1.0 Log Scanner

Navigate to https://cx.rightnow.com/app/my_site_tools.

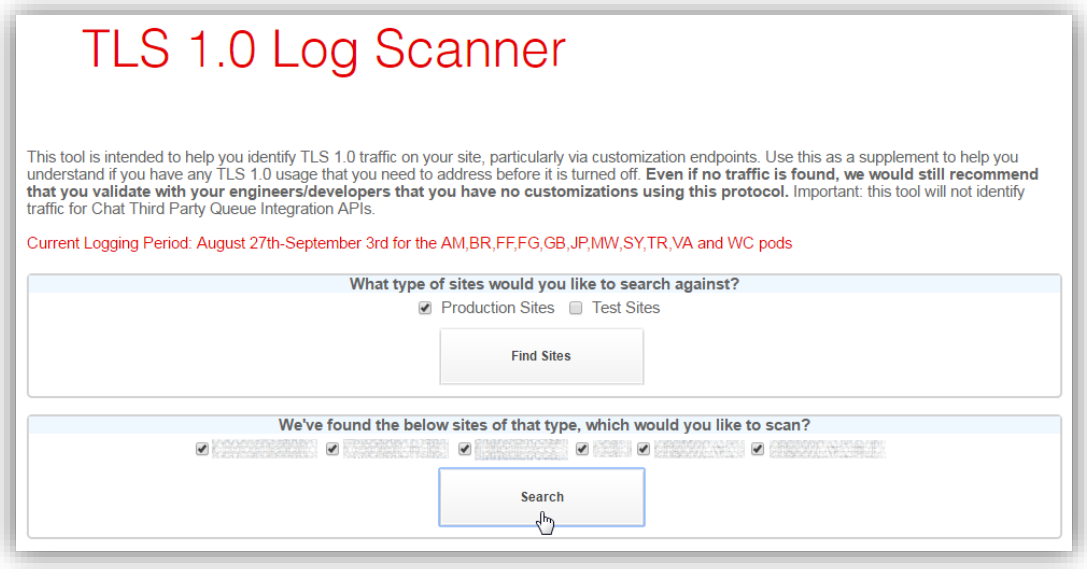
Under **Additional Tools**, select **TLS 1.0 Log Scanner**.



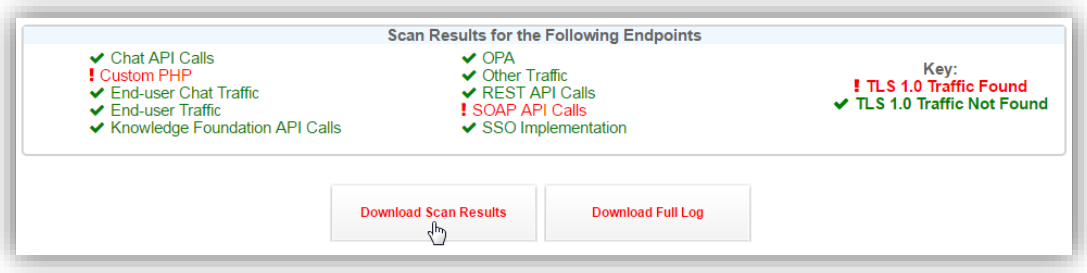
Using the TLS 1.0 Log Scanner

Every Saturday, TLS 1.0 usage data is refreshed in the Log Scanner to include the prior 7 days of TLS 1.0 usage, and older usage data is discarded; the current date range is indicated on-screen. Because data is refreshed weekly, Oracle recommends making use of this tool on a weekly basis for the best chance of identifying and resolving all TLS 1.0 usage on your Oracle Service Cloud instance(s). The Log Scanner is easy to use.

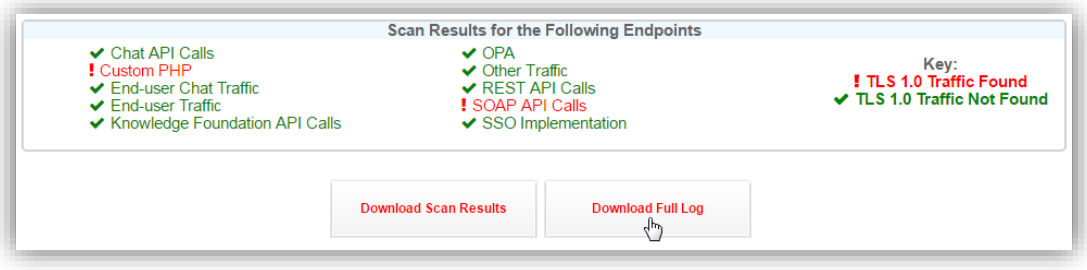
First, choose which types of sites – Production or Test or both – that you wish to scan, and select **Find Sites**. Next, from your listed sites, check the box for each site you wish to scan, and select **Search**.



Review the Scan Results. Oracle looks for various specific patterns within the traffic. If TLS 1.0 usage with a certain pattern is detected, it is indicated on-screen in red. After searching for TLS 1.0 usage, select **Download Scan Results** to receive a CSV file containing those log entries.



To download ALL TLS 1.0 usage, select **Download Full Log**. This reveals the most comprehensive view of TLS 1.0 usage for your selected site(s).



IMPORTANT: ANYTHING present in the downloaded logs indicates TLS 1.0 usage, and **you must remediate it to use a more secure protocol such as TLS 1.2**. See the next section for assistance interpreting log file contents.

Intepreting TLS 1.0 Log Traffic

After downloading the CSV file representing either the Scan Results or the Full Log, open it using Excel or another application capable of handling CSV data.

The CSV file contains five columns described here.

COLUMN	DESCRIPTION
Vhost	This is the virtual host being accessed.
Hits	This is the number of times the Vhost has been accessed during the reporting period.
Source IP	This is the IP address of the source accessing the Vhost.
URL	This is the specific URL endpoint being access from the Source IP.
User Agent	If the agent at the Source IP that is accessing the URL provides any additional information about itself, it will be listed here.

The Log Scanner detects the expressions listed in the table below.

TLS TRAFFIC	EXPRESSION MATCHED IN URL
Chat API Calls	/services/chat_soap
Custom PHP	/php/custom
End-user Chat Traffic	/Chat/chat
End-user Traffic	/app/
Knowledge Foundation API Calls	/kf_soap
OPA	/opa-hub/soap
REST API Calls	/services/rest
SOAP API Calls	/services/soap
SSO Implementation	/ci/openlogin/saml
Other: WebDAV Traffic	/dav/ *(Customer Portal developer access for updating end-user pages)*
Other: End-user Assets	/euf/ *(CSS, images, JavaScript libraries, or other assets)*
Other: Agent Console Traffic	/xml_api/soap_api.php *(TLS 1.0 traffic from the agent console was deprecated as of version 14.2. See Answer ID 8576 for details.)*

NOTE: When you download the Full Log, you may see URLs that are not listed here; the list above is not exhaustive. All TLS 1.0 usage requires your remediation.