Cyber Alarm 3.0

Configuration Guide

and

Instruction Manual

Contents

Introduction

Welcome to Cyber Alarm Antivirus for Salesforce Version 3.0! Starpond Software proudly presents Cyber Alarm Antivirus for Salesforce. Cyber Alarm will allow you to natively scan your Files for malicious code without sending your organizations confidential files out to third party servers for scanning. So, what does this mean to you? This means that your companies files stay inside your Salesforce Org. period. Cyber Alarm has been carefully streamlined and designed and meticulously engineered to do its efficient scans inside of Salesforce for you.

Our motto at Starpond Software is to offer our customers 'Overwhelming Value and Support' and that is exactly what we intend to do to win your business. So, whether it is with our great software like Cyber Alarm or the Cloudpond S3 Connector, or great prices or unprecedented Technical Support, we know you will love our products. So jump on board and let us protect your Salesforce platform from malicious code. We are glad you are here, and please let us know if there is any way we can assist you.

Prerequisites

This guide and installation manual assumes the reader has an existing Salesforce Production or Developer Org. For a full licensed installation, the user must have at least 200 MB of free storage. One should note that the free developer edition from Salesforce only comes with 5 MB of free storage. You will only be able to install the full licensed version of Cyber Alarm into a free developer org if you open a case with Salesforce and ask for additional free developer org storage. You will need to ask Salesforce for a minimum of 200 MB of free storage in the free developer org. The reason for this is that the virus signature load to the Virus Signatures object will consume 153 MB of storage. We also assume the Administrator has general knowledge of computer terms such as virus signatures, batch scans, antivirus, and quarantine.

Background

Salesforce is the worlds most popular Customer Relationship (CRM) Management system. It is used world-wide for its CRM capabilities as well as a case management system (Service Cloud). With the advent on its capabilities for Customer Communities and Partner Communities it is now a popular platform for a great way to connect with customers and partners. However, Salesforce does not scan file attachments for malicious code and instead relies on third party vendors to accomplish this capability for its platform.

Starpond Software introduced Cyber Alarm in September of 2016 as the first native capability to scan files and attachments for malicious virus signatures. The Starpond Software development team for Cyber Alarm has a 20 year history of Software Development for Malicious code detection, Cyber Security and Computer Forensics. Fast forward to 2020 and we have proudly released Cyber Alarm 3.0 which offers several new capabilities to include batch scans and new optional attack vector blocking capabilities and MD5 hashing cross checks for known existing malicious files. Cyber Alarm allows your System Administrator to be in full control of everything. There is no need to send your files outside the Salesforce Org for virus

checking, we keep it in your Salesforce org. with our efficient streamlined algorithms.   The only time your Salesforce Org will communicate with a 3ʳᵈ party server is when it downloads the latest antivirus signatures on demand by pressing the button in the settings tab.

Installation Steps

Step 1 Begin Installation

While logged in to the destination Salesforce Org, go to the AppExchange at URL:

https://appexchange.salesforce.com/listingDetail?listingId=a0N3A00000DqDF1UAN

Choose the green 'Get It Now Button'
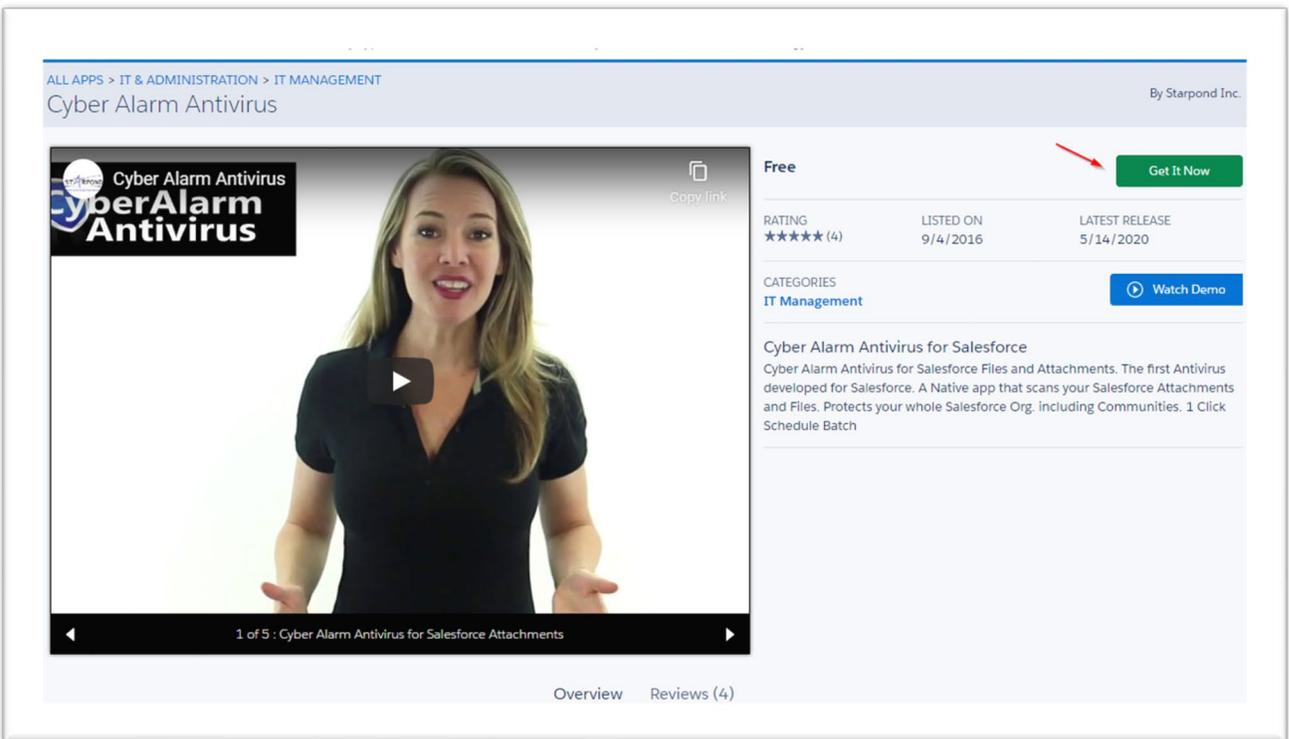
Figure 1 – Use the 'Get It Now' Button in while on the Cyber Alarm AppExchange Page.

Step 2 Ensure only Admins can access the Cyber Alarm App

Install Cyber Alarm for Admins Only. This will ensure only Salesforce Admins can access the controls of the Cyber Alarm App.
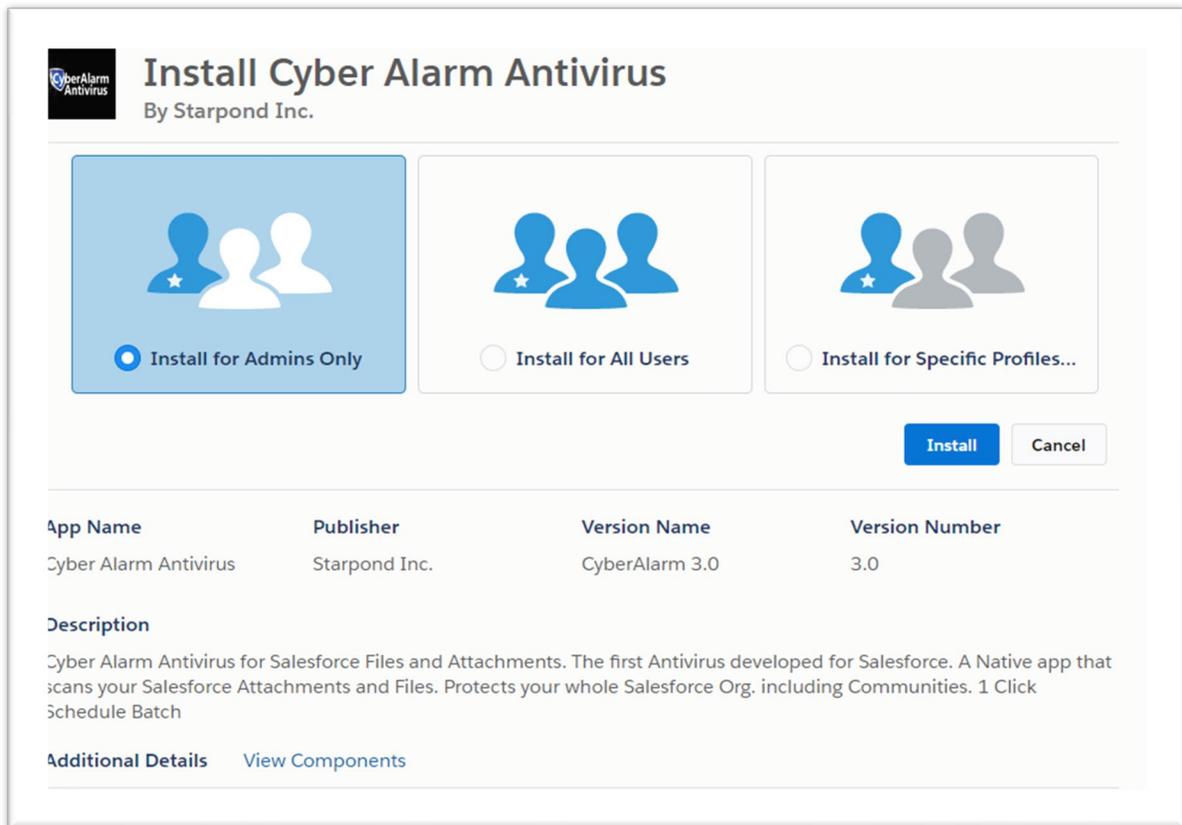
Figure 2 – Install Cyber Alarm app so that only Admins have access

Step 3 Review the Package Components and Install

You can review the package components (optional) of what will be installed with Cyber Alarm.

You will also need to grant access to s3.amazonaws.com to be able to import new virus signatures.

Updating virus signatures is on demand and happens when your Admin presses the button. Updating virus signatures is not automatic.

Figure 3 – Review the components that are included with Cyber Alarm

Figure 4 – By click on View Components you can see the components which will be installed
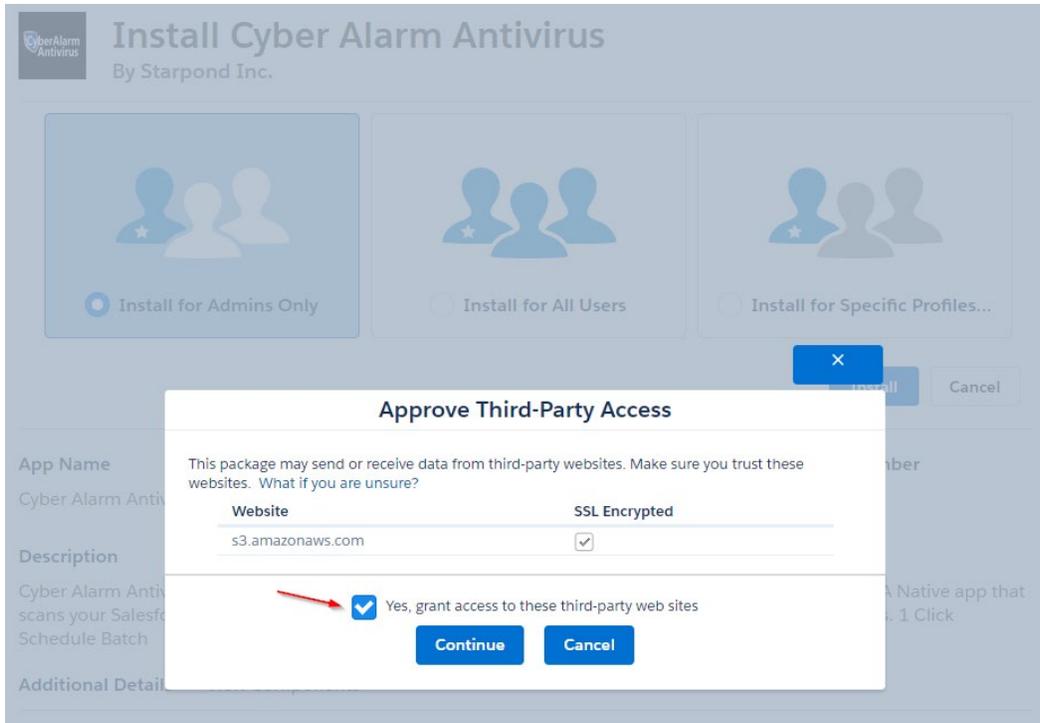
Figure 5 – You must grant access to the Cyber Alarm AWS website to be able to update your virus signatures.

Cyber Alarm will begin its installation into your Salesforce Org.
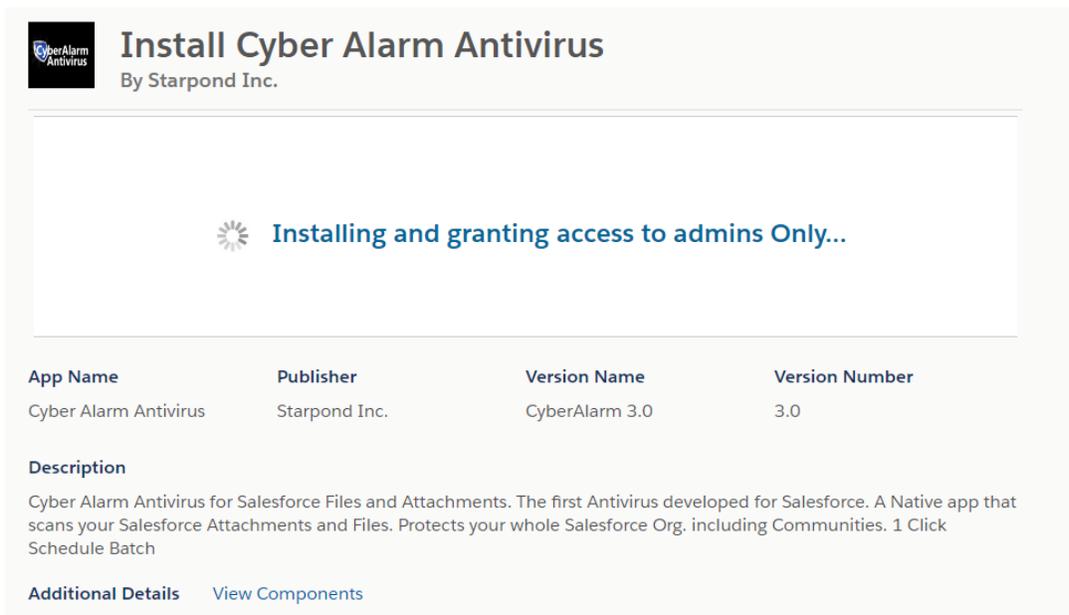
Figure 6 – Cyber Alarm will begin it's installation into your Salesforce Org.

When Cyber Alarm has completed it's installation you will see the confirmation screen. Click the 'Done' button.

Figure 7 – Installation is complete confirmation screen

Step 4 Post Install Setup

Once you are back in your Salesforce Org and the installation has completed you will need to go to the New Cyber Alarm App
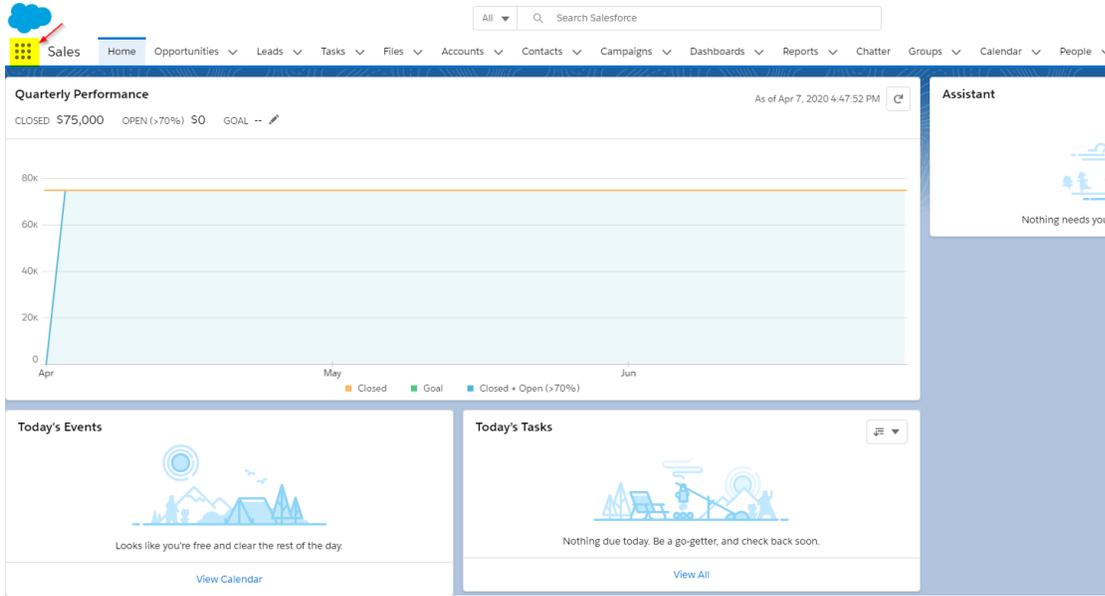
Figure 8 – In Lightning Experience click on the nine dots
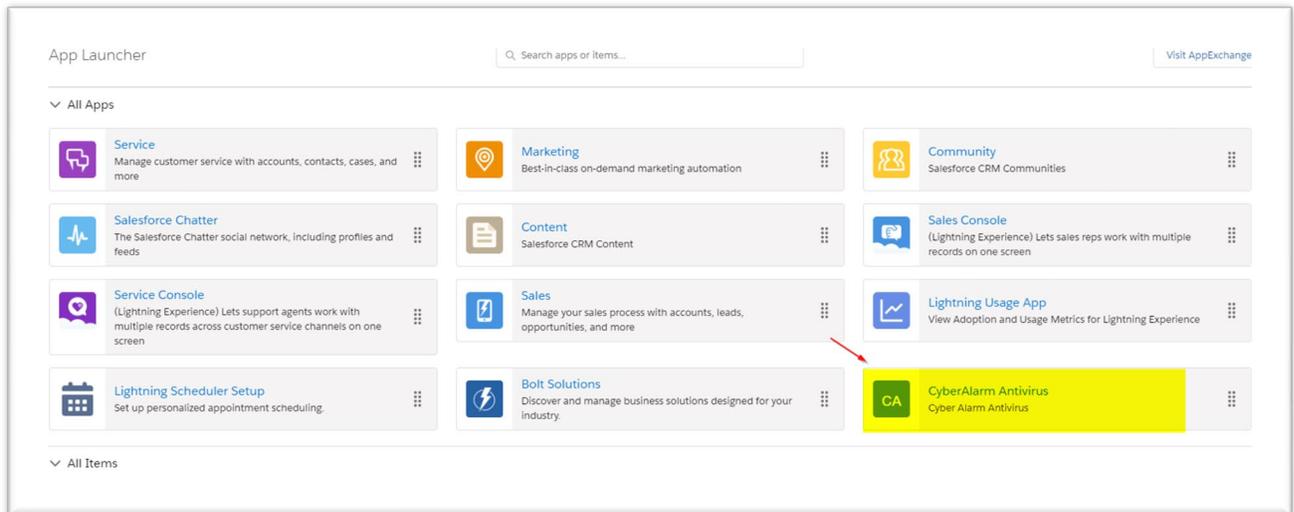
Figure 9 – Choose View All and navigate to the Cyber Alarm App

On the Cyber alarm settings page, you can control the functionality of Cyber Alarm and request a paid license if you choose.
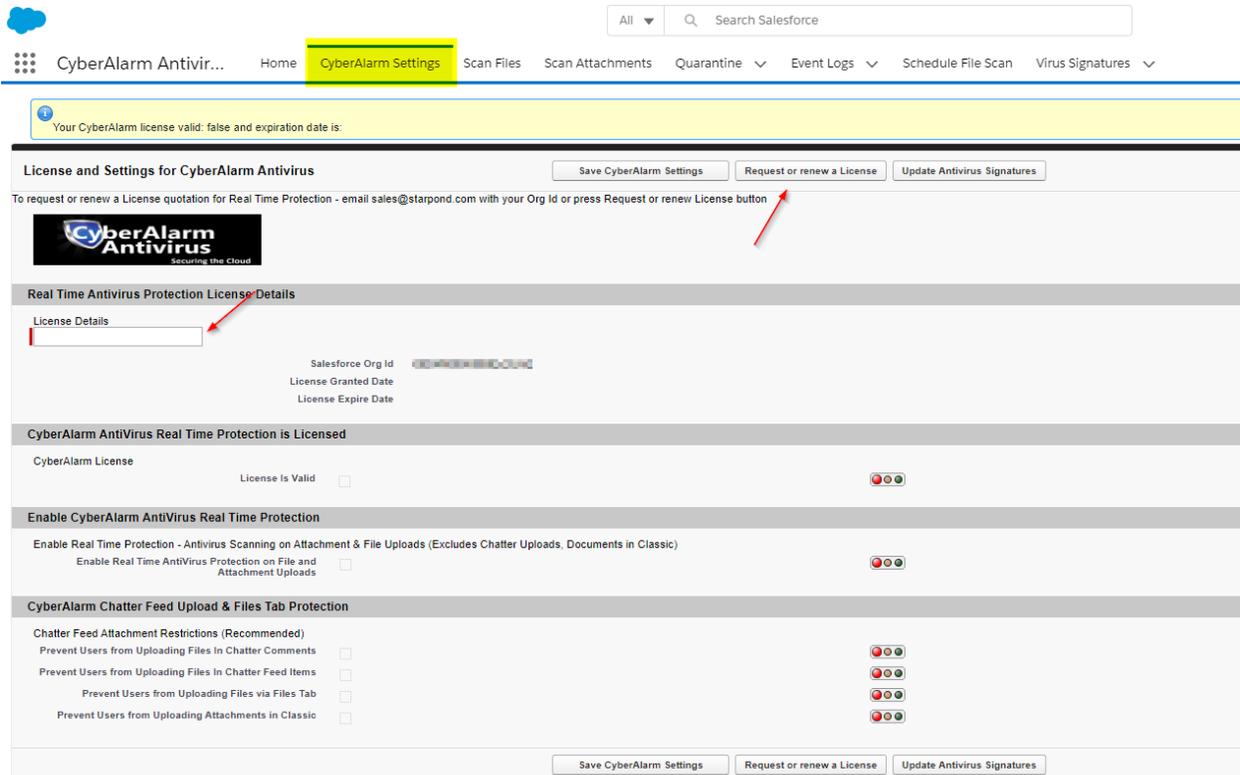
Figure 10 – Cyber Alarm Settings Page

Step 5 Settings to enforce the use of 'Files' with Record Access

Ensure that your Salesforce Org in now saving Attachments as files instead of Attachments.

With Files, there is now the ability to relate files to multiple records, track multiple versions, and view file previews. You can now share a single File with users, groups, or records, providing more control over what is shared. Additionally, it offers version control, collaborates with Chatter, and is optimized for Lightning.

Important: For security reasons Files offer an MD5 Checksum which Cyber Alarm will utilize to ensure the Files MD5 checksum is not matching with one of tens of thousands of known virus signatures, which offers the org better security protection.

Step 5a: Steps to Enable that the Salesforce Org is using Files instead of Attachments:

1. Go to Setup.
2. Go to Salesforce Files (quick find: type "Salesforce Files")
3. Click General setting.
4. Click Edit.
5. ***Check "Files uploaded to the Attachments related list on records are uploaded as Salesforce Files, not as attachments"***
6. Click Save.
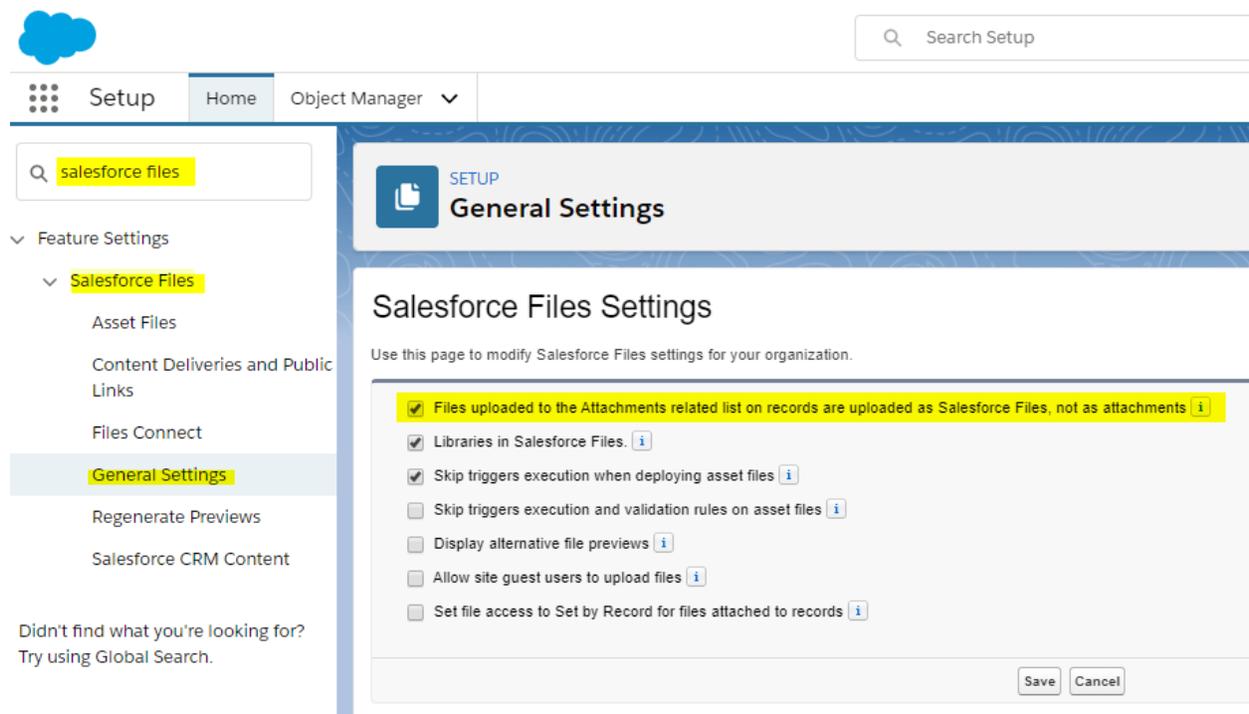
Figure 11 – Enforce the use of Salesforce Files ***Set by Record Access*** in the Salesforce Org.

Step 5 B: Steps to Enable that the Salesforce Org is using Files <u>Set by Record Access:</u>

7. Go to Setup.
8. Go to Salesforce Files (quick find: type "Salesforce Files")
9. Click General setting.
10. Click Edit.
11. ***Check Set file access to Set by Record for Files Attached to Records***
12. Click Save.
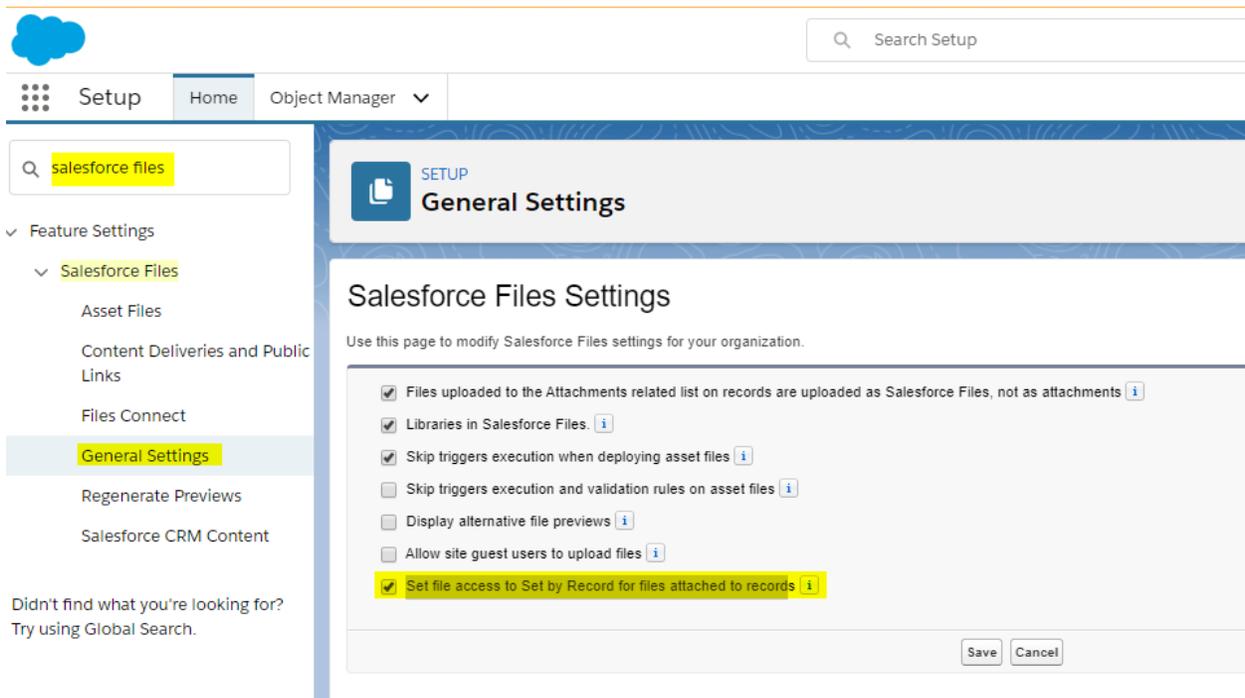
Figure 12 – Set File Access by Record for Files Attached to Records

The reason to change **File Access to by record** is so that the Administrator has Access to all files for Batch Antivirus Scanning as well as access to all files from the Scan Files Page on Cyber Alarm. The important point here is that the Admin who will be using Cyber Alarm has access to all files uploaded so they can be scanned by Cyber Alarm utilities.

Step 6 Using the Cyber Alarm Graphical user Interface

On the Cyber Alarm Scan Files Tab the Admin will be able to search for any file in the Salesforce Org and conduct a antivirus scan. There are several columns to be able to sort the files as well. Keep in mind that Set File Access by Record needs to be enabled in order for the files in the Salesforce org. to show up on this page.

Figure 13 – The Scan Files Tab in Cyber Alarm allows Admins to search for and scan files

Figure 14 – An Admin can click on any file in the list and scan it for a virus. Results displayed above.

Step 7 Batch Scan of the entire Salesforce Org's Files

With Cyber Alarm 3.0 the Admin can now conduct an Batch Antivirus scan the entire org's Files.

With our simple one step batch scan an Admin can schedule a batch to run on one of several timed intervals. It should be noted that if hourly intervals are chosen the batch will on the hour of the beginning of the next hour.

Step 8 Noting Quarantined Files

Files that are found to have been positively identified as containing a virus will be quarantined by Cyber Alarm. Quarantined Files can be found in the Salesforce Recycle Bin for 15 days.

Cyber Alarm Sales and Support

Email: support@starpond.com

Phone: 703-486-6258

Cyber Alarm Licensing for Full Version

Email: sales@starpond.com

Phone: 703-486-6258