ShareFile Uploads and Symantec DLP Setup

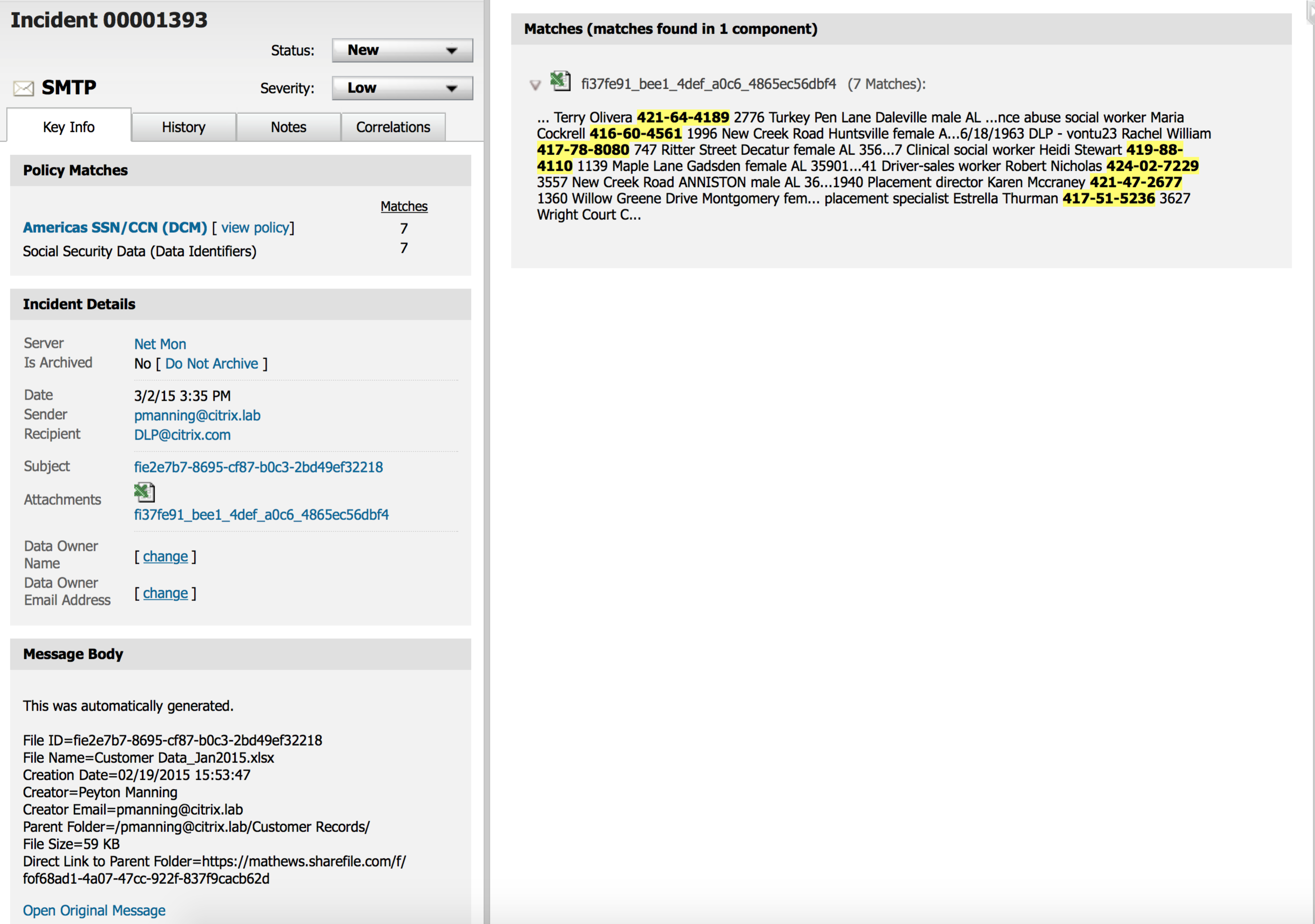
## These are instructions for setting up ShareFile and Symantec DLP to inspect all files being uploaded to on-prem data.

**USE CASE:**

Customers would like to gain visibility of sensitive data (PII, PHI, Company Confidential, etc.) that has been uploaded to ShareFile near real-time.

**SOLUTION:**

Use PowerShell script created by Cameron Erens and Brian Mathews to send all files to DLP for inspection as they are uploaded into ShareFile to determine if any files violate DLP policy.

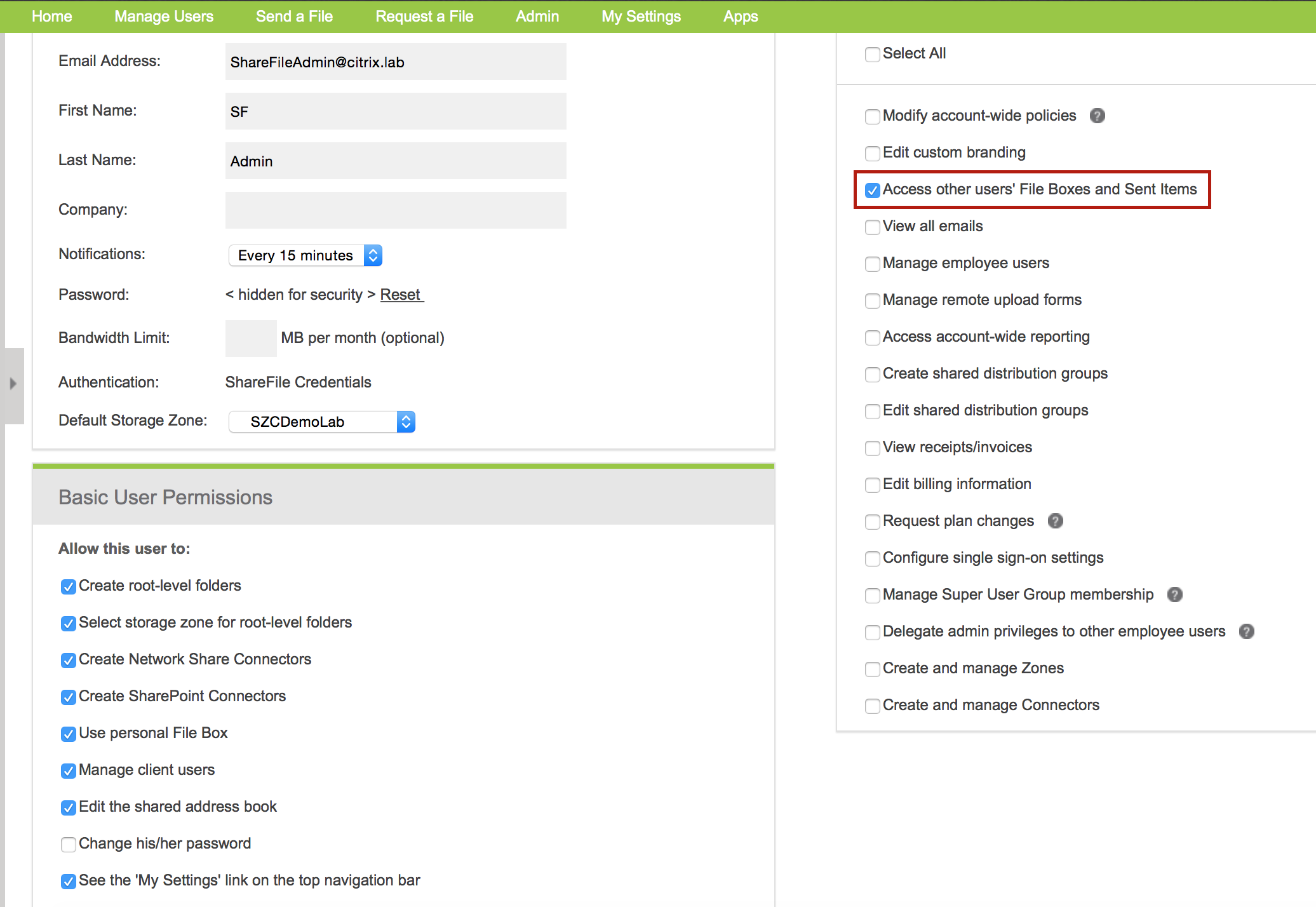


\* Symantec DLP incident shown with details of the file uploaded into ShareFile.

**Prerequisites**:

Create a ShareFile Service Account (member of the Super User Group), may use existing if desired:

1. Log in to ShareFile with an account that has “Create Employee” privileges
2. Navigate to Manage Users -> Create Employee
   1. Example: [ShareFileAdmin@citrix.lab](mailto:ShareFileAdmin@citrix.lab)
   2. At a minimum this user needs “Access other users’ File Boxes and Sent Items”
3. This user **must** be a member of the **super user group** (see [*How do I add members to the super user group*](https://support.citrixonline.com/en_US/sharefile/help_files/SF050008%3Ftitle=Super+Users))



***Disclaimer:***

This document assumes that Symantec DLP has been installed to the default path **C:\SymantecDLP**. If Symantec DLP is not installed to the default path, then you will need to substitute your own path instead of C:\SymantecDLP when referenced in this document.

**\* Please note a working knowledge of PowerShell execution policies and Symantec DLP is required.**

**Tasks for the ShareFile StorageZone Controller (SZC):**

* Please note that items in **bold** may need be modified or created.
* Must be logged in as an Administrator.

1. Navigate to c:\inetpub\wwwroot\Citrix\StorageCenter\
   * + Edit the “**AppSettingsRelease.config**” file
     + Set **QueueSDKRestricted** to 0:

<add key="QueueSDKRestricted" value="0"/>

1. Setup the AV queue:
   1. On the StorageZone Controller(s), edit C:\inetpub\wwwroot\Citrix\StorageCenter\Tools\SFAntiVirus\**SFAntiVirus.exe.config** with the following key values from *your* SZC configuration (ShareFileURL, ZoneName and StorageLocation):

Use SF Config page to validate values

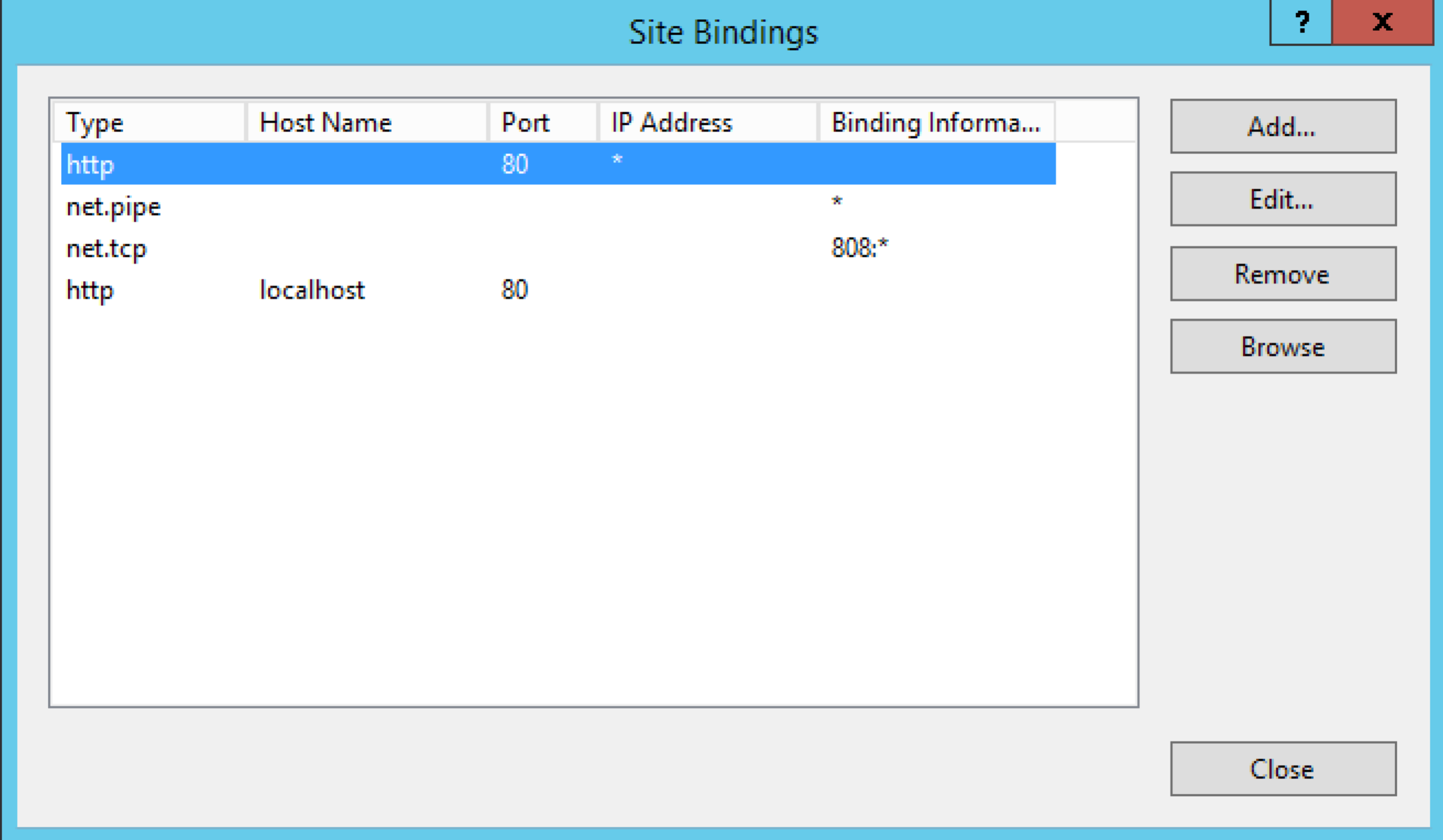
Items in **bold** need to reflect your setup:

* + - <add key="ShareFileUrl" value="https://**demo**.sharefile.com" />
    - <add key="QueueSdkUrl" value="http://localhost/rest/queue.aspx" />
    - <add key="ZoneName" value="**SZCDemoLab**" />
    - <add key="StorageLocation" value="**\\storagezone\ShareFileData**" />
  1. From a Windows command (SFAntiVirus Directory) prompt, run:
     + SFAntiVirus -register **user@companyname.com** **ShareFilePassword**

<Replace bold items with ShareFileAdminLoginEmail and Password>

* + - Validate that the following folder “914DF171-825A-4E0A-B622-384C0778386F” was created by navigating to C:\ShareFileData\Queue

1. To ensure that the Enforce server will be able to connect to the queue on the StorageZones Controller server:
   * + Within IIS Manager, make sure that in ‘Edit Bindings’ for the Default Web Site, port 80 is listening on all IPs.



1. The lookup script requires some StorageZones Controller libraries, to read items from the upload / AV queue.
   1. From the StorageZones Controller server, **copy** the C:\inetpub\wwwroot\Citrix\StorageCenter\Tools\Disaster Recovery folder to **C:\SymantecDLP**\Protect\Plugins on the Enforce Server
   2. On the Enforce server, create a new folder called **sf\_bin**: **C:\SymantecDLP**\Protect\Plugins\**sf\_bin**

* From the StorageZones Controller server, **copy** the contents of C:\inetpub\wwwroot\Citrix\StorageCenter\bin folder to **C:\SymantecDLP**\Protect\Plugins\**sf\_bin** on the Enforce Server
  1. From the Enforce server, edit the **C:\SymantecDLP**\Protect\Plugins\Disaster Recover\**Recovery.psm1** to specify the absolute path to the libraries and to specify the StorageZones Controller name or IP from which the upload / AV queue will be pulled:

Example values:

* + *Add-Type -Path "****C:\SymantecDLP\Protect\plugins\Disaster Recovery\****LitJson.dll”*
  + *Set-Variable -Name QueueHost -Value “****storagezone****"*
  + *Set-Variable -Name QueuePort -Value “80"*
  + *Import-Module* ***C:\SymantecDLP\Protect\plugins\sf\_bin\****ShareFile.Libraries.dll*

# Additional DLP Setup (must be a DLP Admin):

***Install New Detection Server – Network Monitor***

Although this is *optional* it is recommend to set up a separate **Network Monitor** Detection Server. This instance could be virtualized as long as you have a dedicated NIC to talk with the Enforce Server.

1. Must share the **Drop** folder on this Detection Server (C:\Drop) with the Enforce Server.
2. From the Enforce Server navigate to the directory to verify access: \\detectionserver\C$\drop

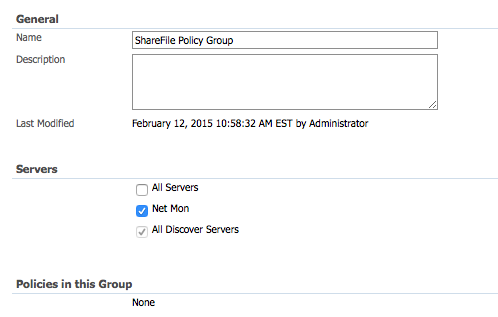
***Create a ShareFile Policy Group <Optional depending on how DLP is deployed>***

*This will be used for detecting ShareFile only incidents. Be sure Policies are added to this group.*

1. Within the DLP Enforce console navigate to **System > Policy Groups**
2. Click **Add**



1. Name: ShareFile Policy Group
2. Select appropriate **Server** from list to deploy ShareFile only policies (mentioned in the pre-reqs)



1. Click **Save**

***Setting up PowerShell to run on the Enforce Server***

1. PowerShell **4.0** must be installed and running. If the Enforce server is running a version of Windows earlier than Windows 2012, then install PowerShell 4.0 (by installing [Windows Management Framework 4.0](http://www.microsoft.com/en-us/download/details.aspx%3Fid=40855))
2. On Enforce server, install [ShareFile PowerShell snap-in](https://github.com/citrix/ShareFile-PowerShell/releases) (run installer)

* Validate that the following folder “C:\Program Files\**ShareFileSnapIn\_Installer**” was created.

1. You must perform a manual login to ShareFile for the first time. This stores the OAuth tokens that will allow access to ShareFile to a local file.

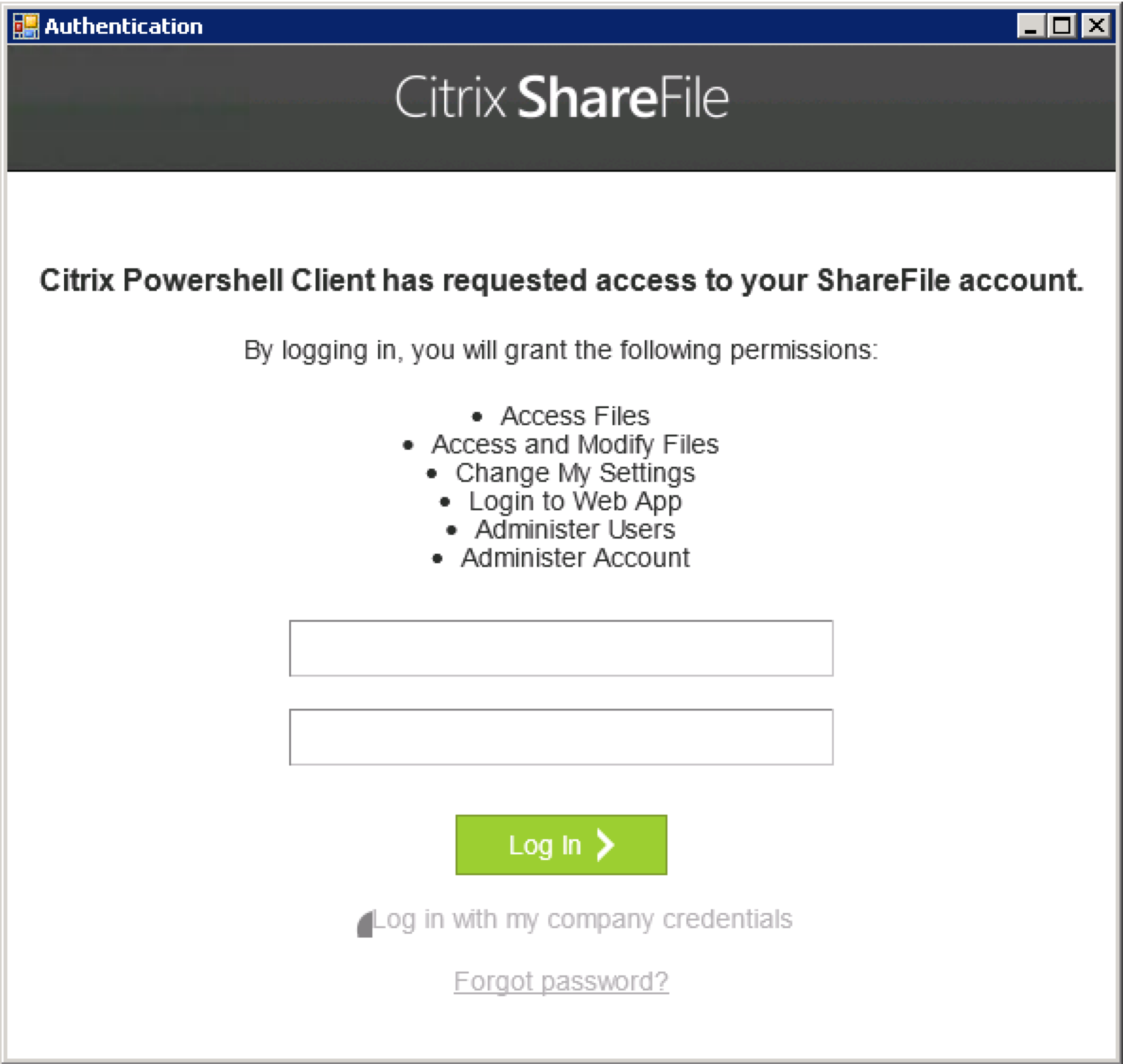
Open PowerShell from the Enforce Server and execute the following 3 lines:

Add-PSSnapin sharefile

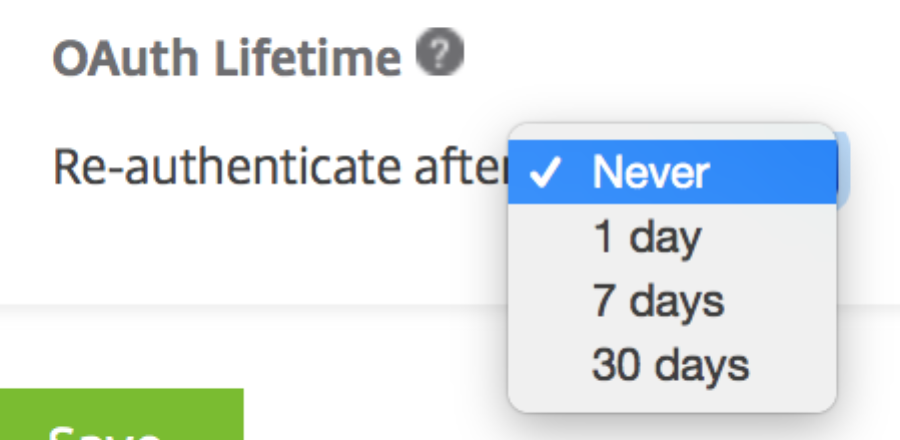
$login = "**C:\SymantecDLP**\Protect\plugins\SFPS-login.sfps"

$sfClient = new-SfClient -Name $login

1. Enter ShareFile credentials (previously discussed in the prerequisites):



1. Check OAuth Lifetime setting within your ShareFile account. The default is set to “Never”, however if it is any other value you will need to perform Steps 3 and 4 (above) to re-authenticate after they expire.
2. Log in into your Share Account as an Administrator and Click **Admin** on the top menu bar
3. Select **Advanced Preferences** from the left side bar
4. Expand **Password, Login and Security Policy**
5. Validate you OAuth setting



1. Download the “Monitor\_Uploads\_From\_ShareFile\_Queue\_SYMC\_DLP.ps1” script from <https://github.com/citrix/ShareFile-PowerShell/blob/master/Samples/Monitor_Uploads_From_ShareFile_Queue_SYMC_DLP.ps1> to **C:\SymantecDLP\**Protect\plugins

\* Also the following 3 lines within the script may need to be modified:

Import-Module **'C:\SymantecDLP**\Protect\plugins\Disaster Recovery\Recovery.psm1'

Import-Module **'C:\SymantecDLP**\Protect\plugins\Disaster Recovery\LitJson.dll'

$login = "**C:\SymantecDLP**\Protect\plugins\SFPS-login.sfps"

Finally, read the comments at the end of the script regarding anti-virus scanning and the two options for clearing out the upload queue. This will ensure that when the script is run repeatedly (below we suggest using Windows Task Scheduler), duplicate incidents will not be generated. Choose one of the two options described in the script comments: either have the script run SFAntiVirus.exe, or alternatively, on the last line of the ‘for’ loop before the end brace, add a line to clear out the queue item (it is at this point in the script that the queue item already will have been processed / the corresponding file in persistentstorage scanned by DLP.)

***Create and schedule a task for DLP scans***

1. Start Windows Task Scheduler and in the **Actions** pane click **Create Task**.
2. On the **General** tab, provide a meaningful
   1. **Name** for the task.
   2. Under **Security options**, click **Change User or Group**, and specify a Windows user to run the task. The user must have read access to the ShareFile storage location, full access to **'C:\SymantecDLP**\Protect\plugins’, and full access to the Symantec DLP drop folder.
   3. Select **Run whether user is logged on or not**. Leave the Do not store password check box cleared.
   4. Select **Run with highest privileges**.
   5. From the **Configure for** menu, select the operating system of the server where the task will be run.
3. To create a trigger: On the **Triggers** tab, click **New**. Then, for **Begin the task**, choose **On a schedule** and specify a schedule.
4. To create an **action**: On the Actions tab, click **New**.
5. For Action, choose **Start a program**.
6. For **Program/script**, specify: Powershell.exe
7. For **Add arguments**, specify: -executionpolicy bypass **C:\SymantecDLP**\Protect\plugins\Monitor\_Uploads\_From\_ShareFile\_Queue\_SYMC\_DLP.ps1
8. On the **Settings** tab, for **If the task is already running, then the following rule applies,** choose **Do not start a new instance.**