This document explains the procedure of how to use the security tools and their implementations in real time. All the commands concepts etc., are implemented by me in real time and got certifications on that.

Please do check my LinkedIn profile: https://www.linkedin.com/in/vinay-reddy-donda-36b10a20b/

- This document will cover the different topics of Symantec DLP.
- Identifying and describing the confidential data.
- Create policy groups:
- Configure a policy for PII Detection, PCI compliance.
- Configure a policy to protect the confidential document, protect the source code, form recongintion:
- Export policies for use at the Disaster Recovery Site
- Configure the optical character reconigantion.
- Locating the confidential data stored on the premises and on the cloud.
- Scan endpoint computers for confidential data.
- Scan server for confidential data using EMDI
- Configure a global policy for PII Compliance.
- Understanding how confidential data is being used.
- Use network prevent for email to monitor SMTP Messages.
- Monitor endpoint activity- Email, Monitor Endpoint activity – Third party apps
- Monitor end point activity copy/paste, Educating users to Adopt data Protection practices.
- Configure Email Notifications., Configure the on screen notifications.
- Preventing unauthorized exposure of confidential data.
- Testing Optical character recognition(OCR) and “HIPAA and HITECH (including PHI)” Policy.
- Configure Endpoint blocking, Scan and quarantine files on a server file share target.
- Scan and Quarantine files on a endpoint target.
- Remediating the data loss incidents and tracking risk reduction:

- User reports to track risk Exposure and Reduction.

- Define Incident statuses and incident groups.
- Configure and Use smart responses, Schedule and send reports.
- Enhancing data loss preventions with Integrations.

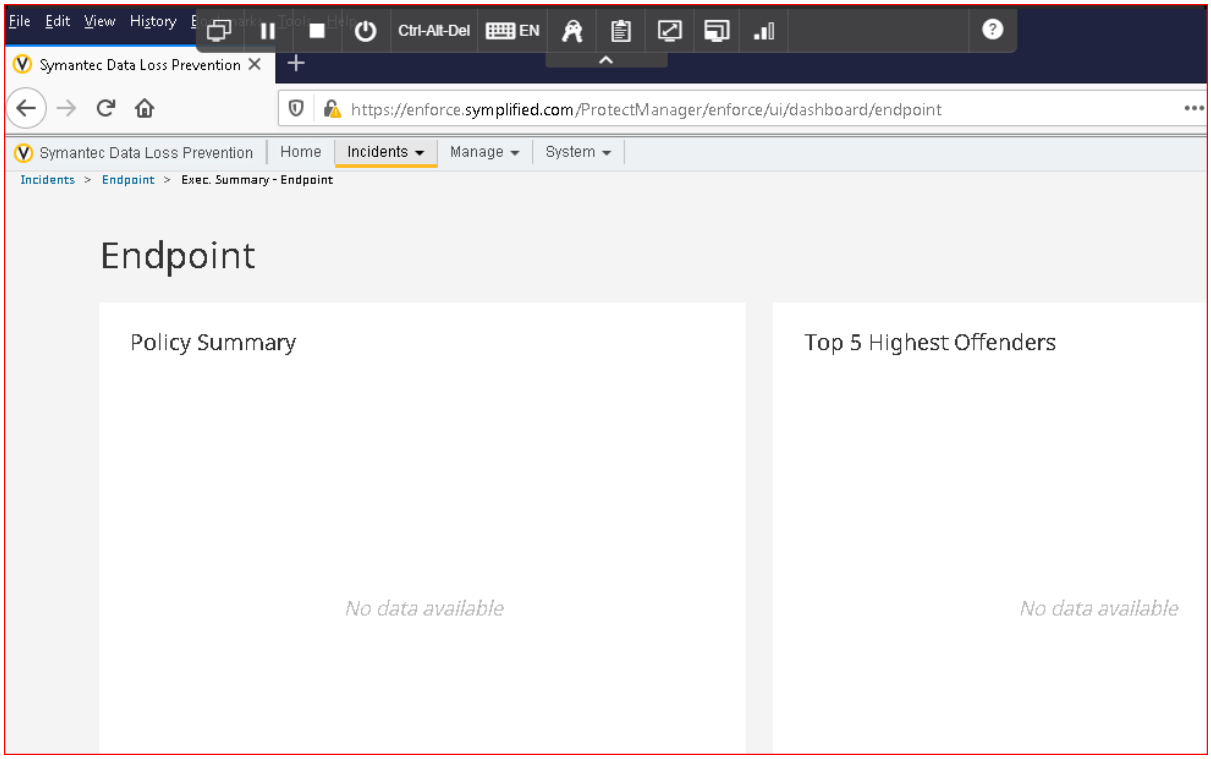
Vinay Kumar Reddy Donda dondavinayreddy@gmail.com

Lab 1:

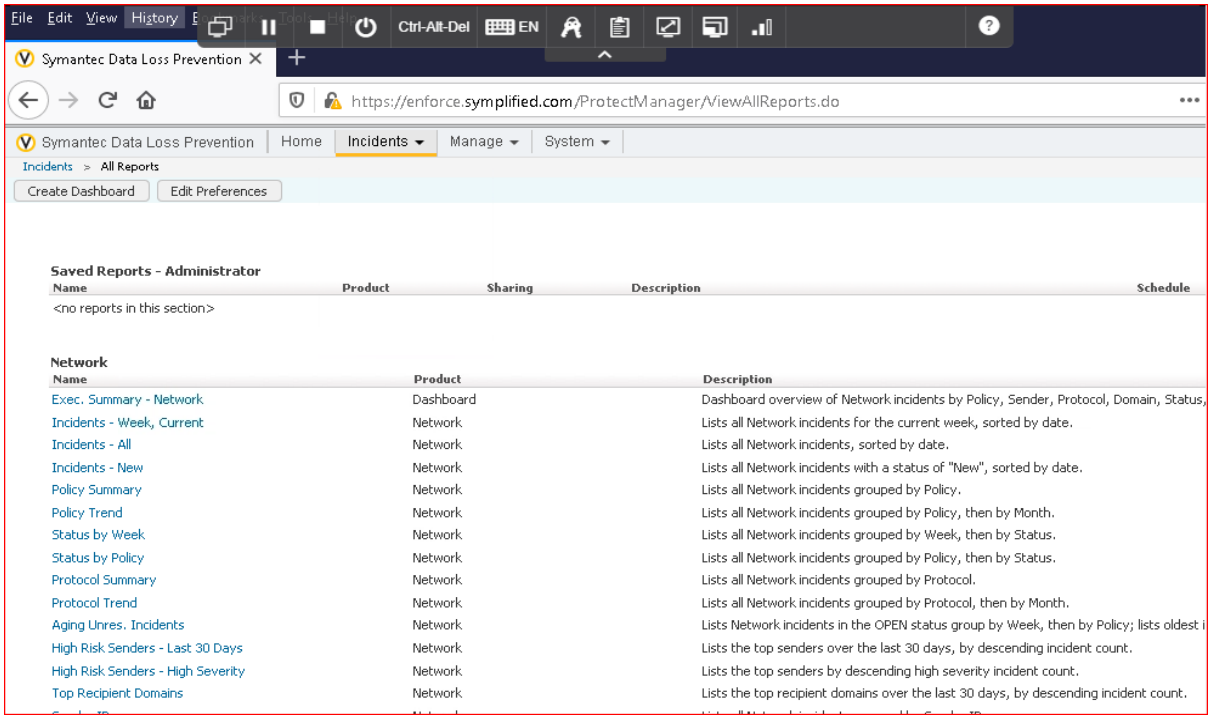
Identifying and describing the confidential data.

Exercise 1:

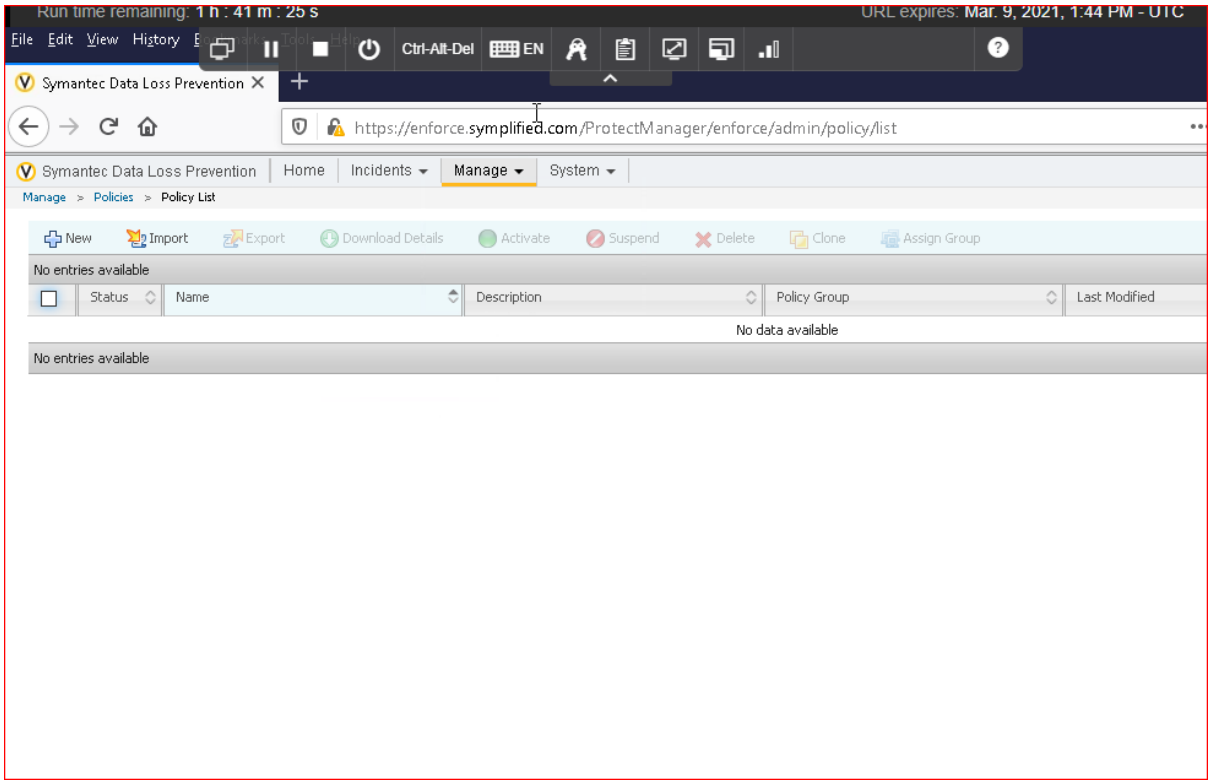
Tour of enforce console.



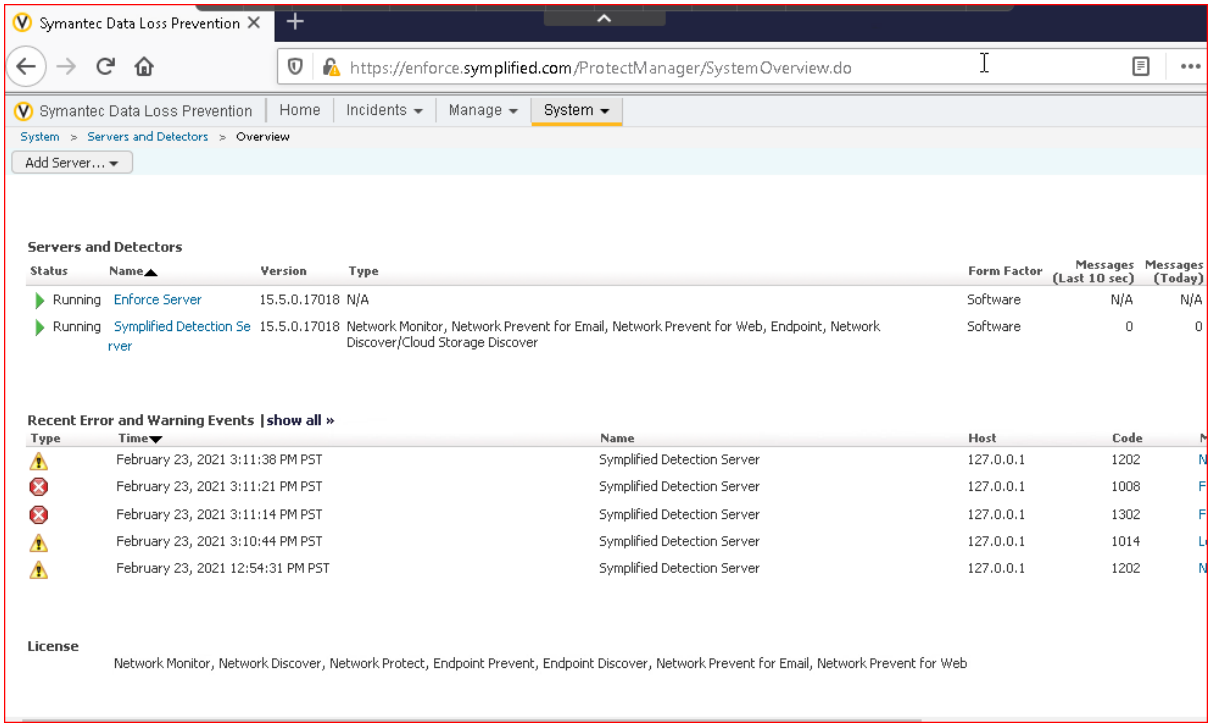
Home tab this contains few built-in reports and dashboards.



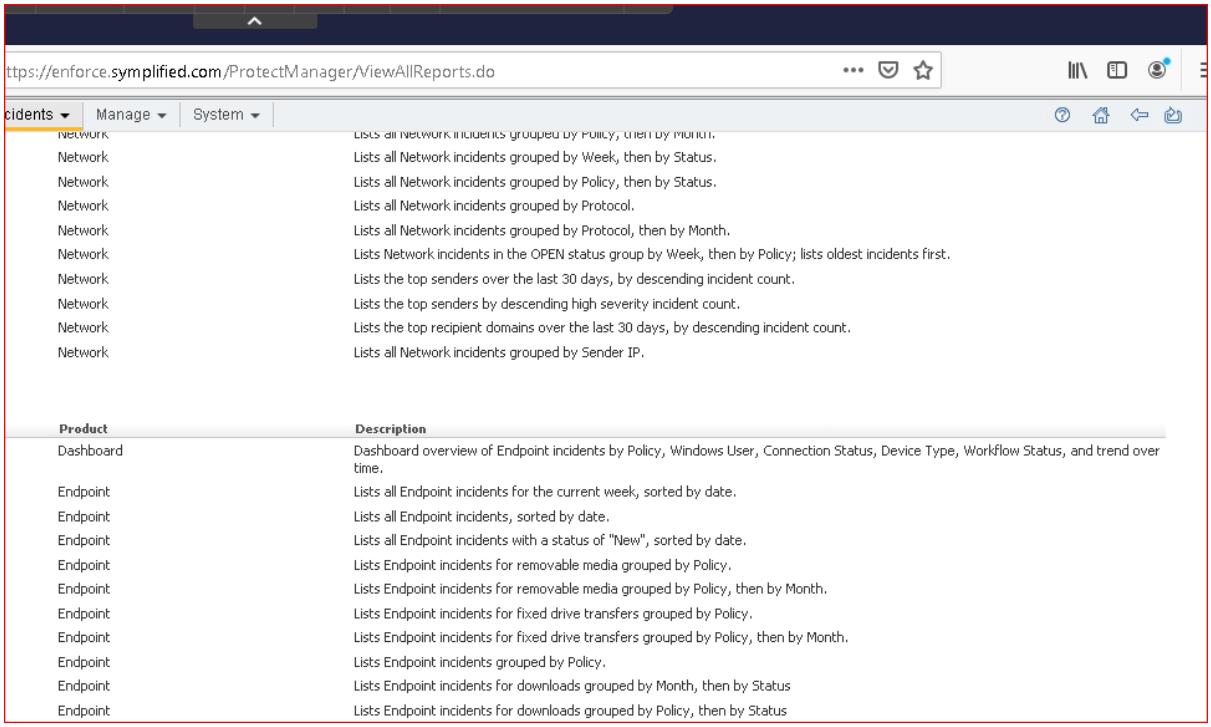
Incident tab this displays the list of reports and incident list for each vector.



Manage tab this is where we add the policies and also says about data profiles and discover scanning.



System tab it is where system wide configuration is done and we can view the status of the enforce server, detection serves , endpoint agents and so on. It is also where the user roles, and permissions are configured.



On the top right corner first symbol indicates the help

Second symbol indicates that whenever we click on that button whatever the console we are using at that time it will become the home screen.

Third symbol indicates going to previous console

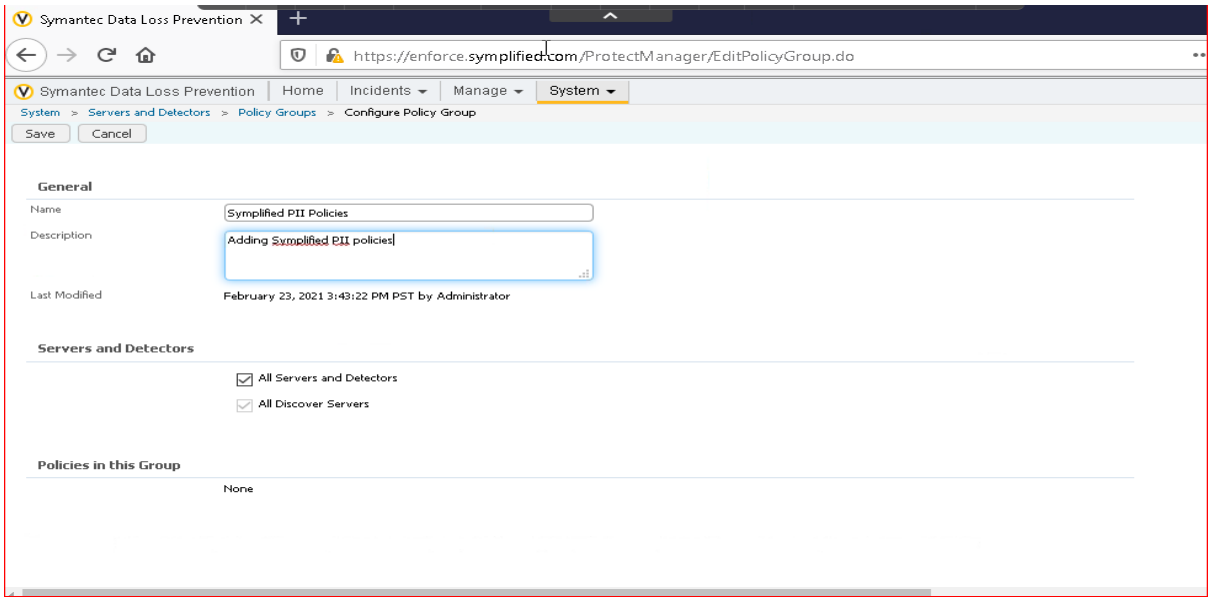
Fourth symbol indicates Refresh of the console

Vinay Kumar Reddy Donda dondavinayreddy@gmail.com

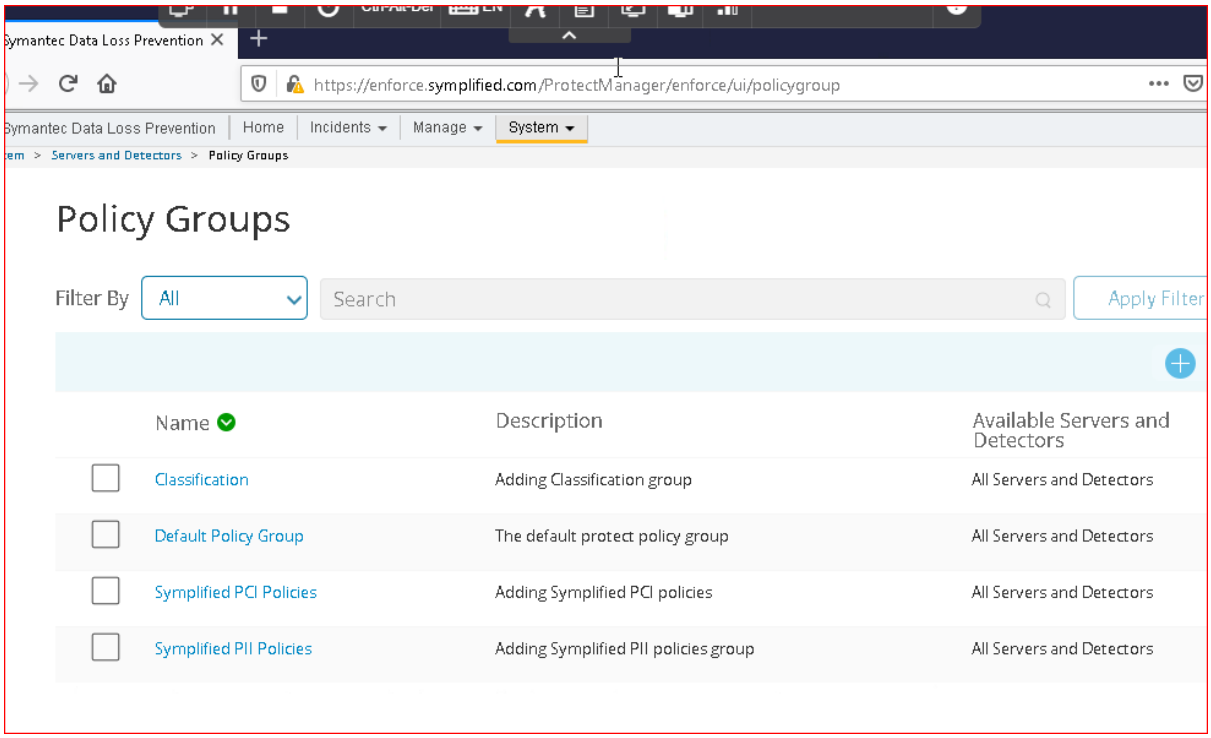
Exercise 2:

Create policy groups:

Policy groups allows us to group similar policies and allows us to detect whether which policy should be used for better data security and avoiding sensitive data loss.



Adding Symplified PII Policies group.



Similary I added Symplified PCI policies and classification group Default Ploicy group need not be added it comes by default.

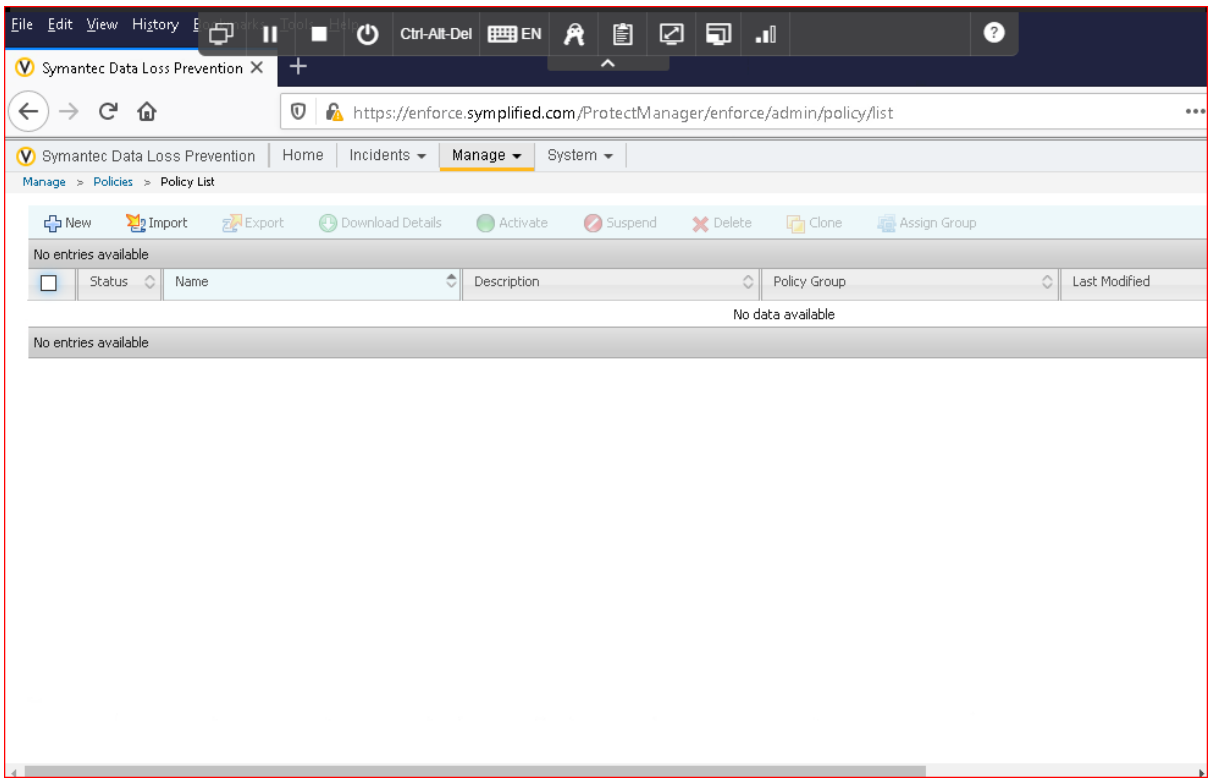
Vinay Kumar Reddy Donda dondavinayreddy@gmail.com

Exercise 3:

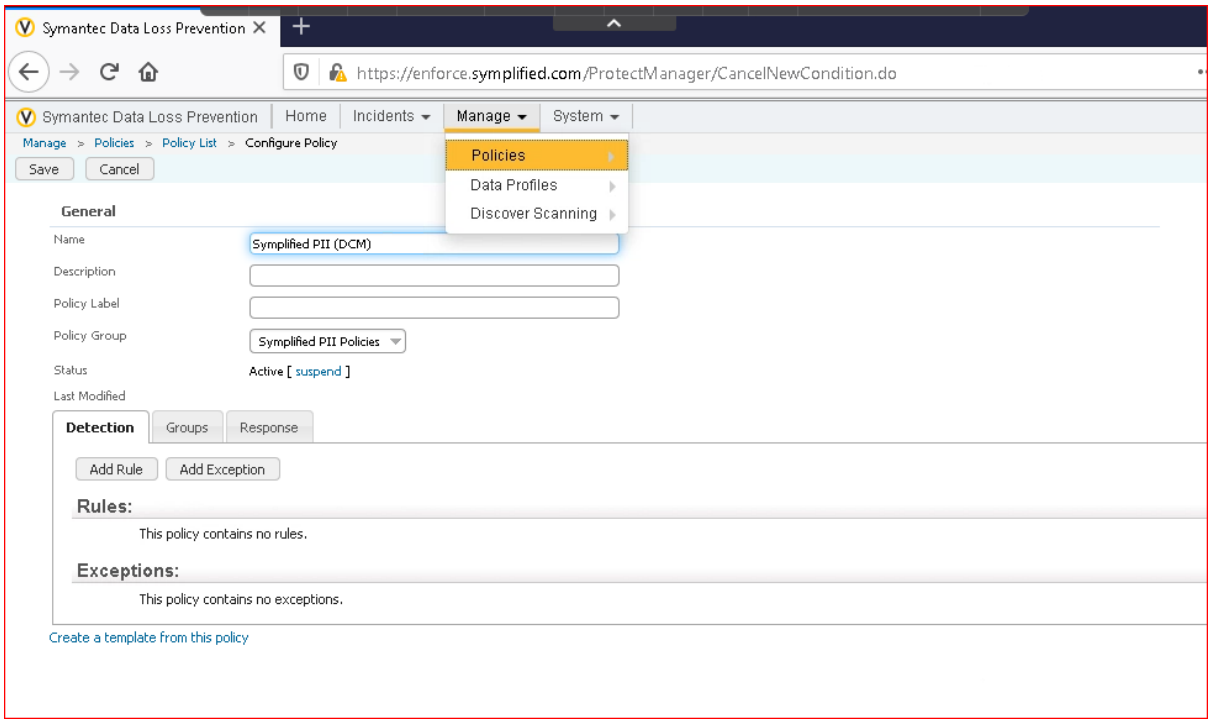
Configure a policy for PII Detection:

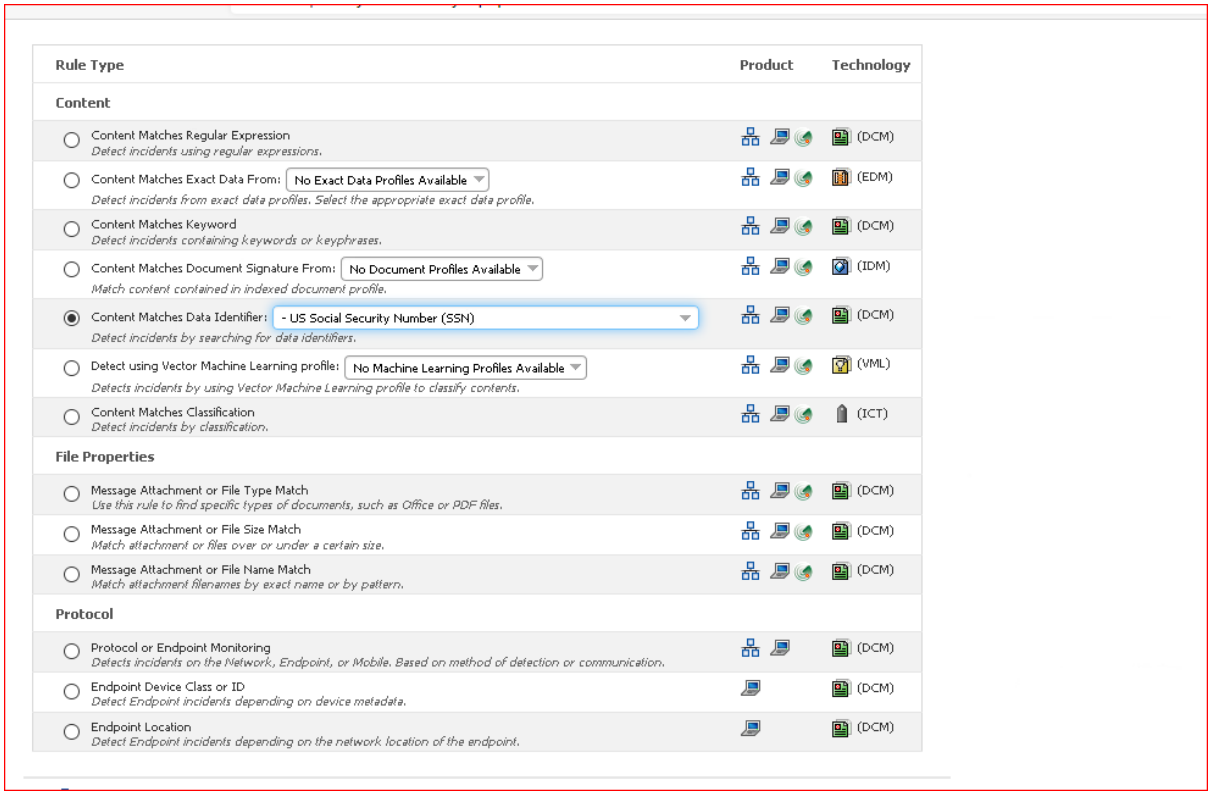
PII – Personally identifiable information.

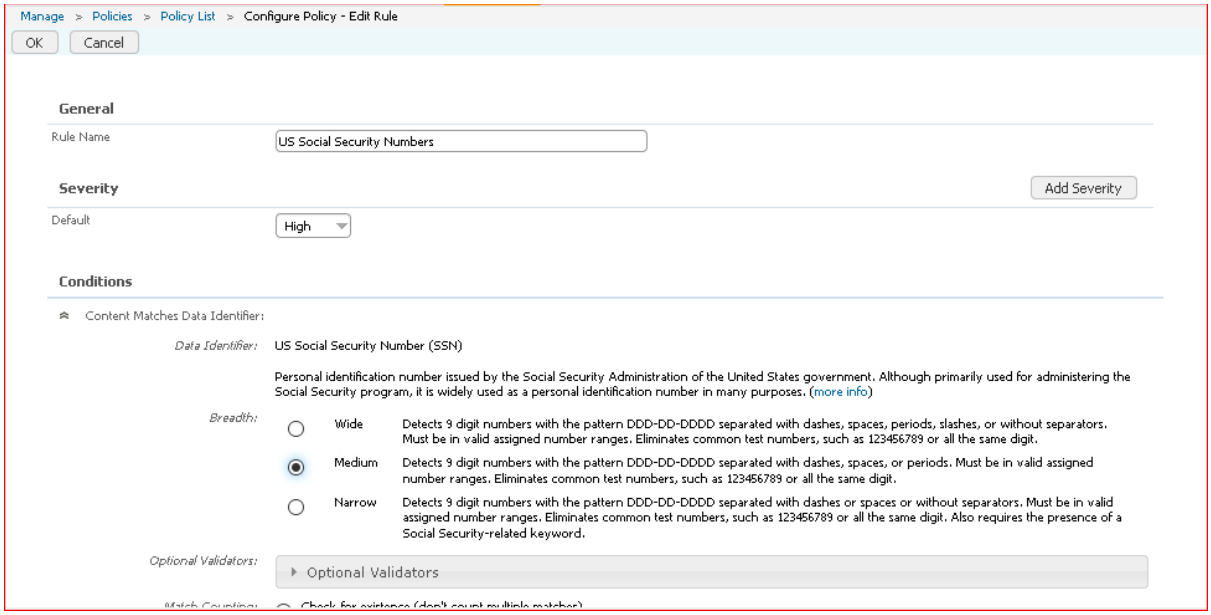
We are creating the policy using the described content matching (DCM) to detect where the PII data is used or stored.

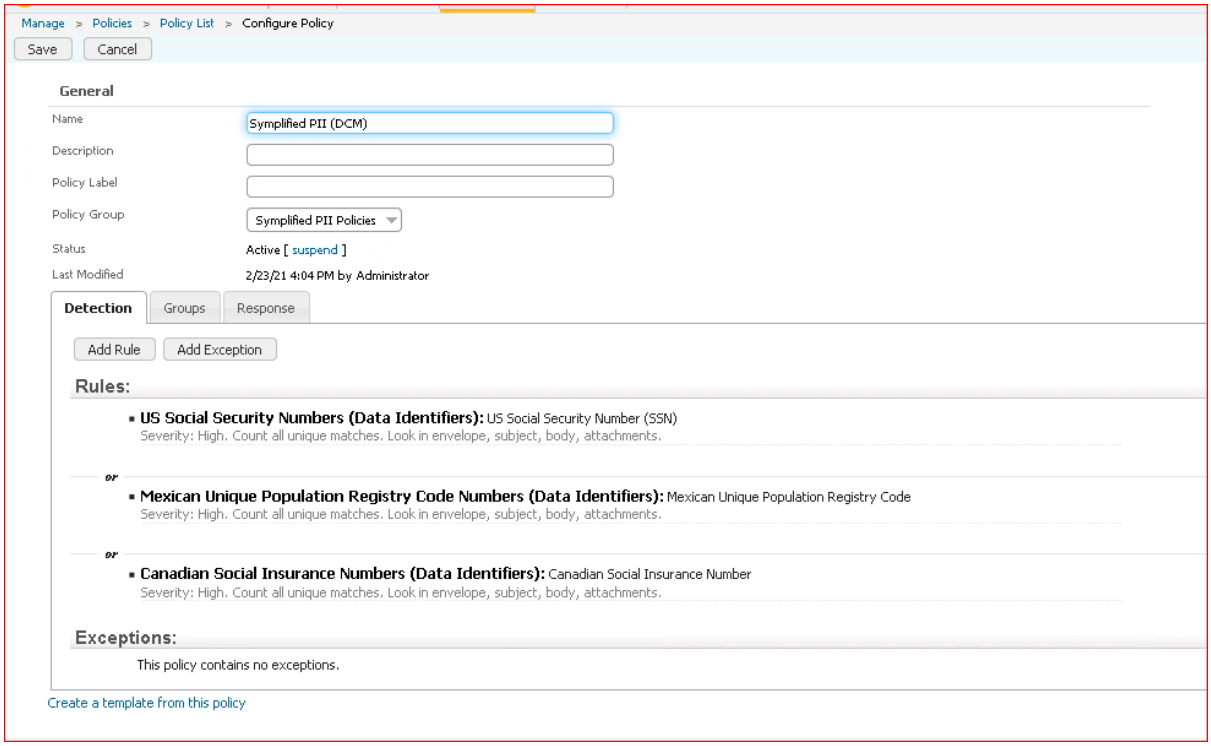


Adding the new policy in the list by clicking new in the console.

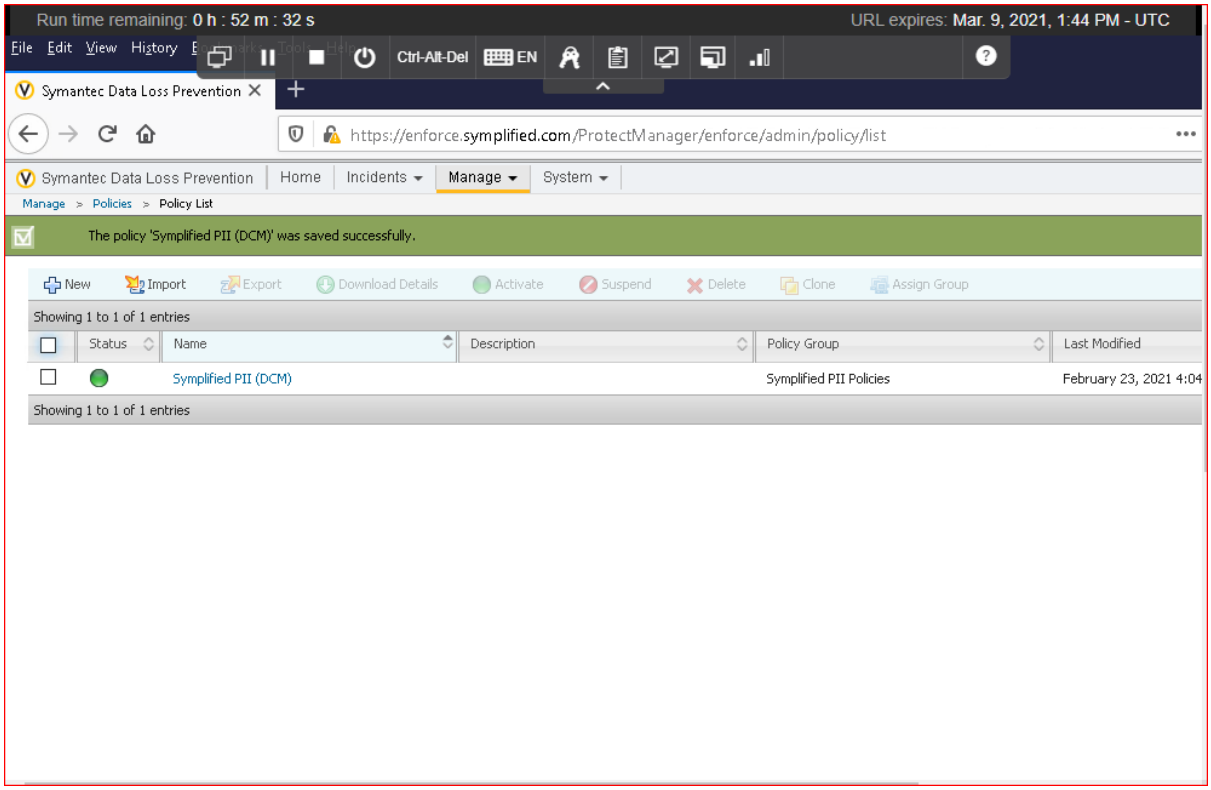



Rule Type
Product
Technology
Content
Content Matches Regular Expression
Detect incidents using regular expressions.
(DCM)
Content Matches Exact Data From:
No Exact Data Profiles Available
Detect incidents from exact data profiles. Select the appropriate exact data profile.
(EDM)
Content Matches Keyword
Detect incidents containing keywords or keyphrases.
(DCM)
Content Matches Document Signature From:
No Document Profiles Available
Match content contained in indexed document profile.
(IDM)
Content Matches Data Identifier:
- US Social Security Number (SSN)
Detect incidents by searching for data identifiers.
(DCM)
Detect using Vector Machine Learning profile:
No Machine Learning Profiles Available
Detects incidents by using Vector Machine Learning profile to classify contents.
(VML)
Content Matches Classification
Detect incidents by classification.
(ICT)
File Properties
Message Attachment or File Type Match
Use this rule to find specific types of documents, such as Office or PDF files.
(DCM)
Message Attachment or File Size Match
Match attachment or files over or under a certain size.
(DCM)
Message Attachment or File Name Match
Match attachment filenames by exact name or by pattern.
(DCM)
Protocol
Protocol or Endpoint Monitoring
Detects incidents on the Network, Endpoint, or Mobile. Based on method of detection or communication.
(DCM)
Endpoint Device Class or ID
Detect Endpoint incidents depending on device metadata.
(DCM)
Endpoint Location
Detect Endpoint incidents depending on the network location of the endpoint.
(DCM)


Manage > Policies > Policy List > Configure Policy - Edit Rule
OK
Cancel
General
Rule Name
US Social Security Numbers
Severity
Add Severity
Default
High
Conditions
Content Matches Data Identifier:
Data Identifier:
US Social Security Number (SSN)
Personal identification number issued by the Social Security Administration of the United States government. Although primarily used for administering the Social Security program, it is widely used as a personal identification number in many purposes. (more info)
Breadth:
Wide
Detects 9 digit numbers with the pattern DDD-DD-DDDD separated with dashes, spaces, periods, slashes, or without separators. Must be in valid assigned number ranges. Eliminates common test numbers, such as 123456789 or all the same digit.
Medium
Detects 9 digit numbers with the pattern DDD-DD-DDDD separated with dashes, spaces, or periods. Must be in valid assigned number ranges. Eliminates common test numbers, such as 123456789 or all the same digit.
Narrow
Detects 9 digit numbers with the pattern DDD-DD-DDDD separated with dashes or spaces or without separators. Must be in valid assigned number ranges. Eliminates common test numbers, such as 123456789 or all the same digit. Also requires the presence of a Social Security-related keyword.
Optional Validators:
Optional Validators



In this we added the rules for DCM which identifies the sensitive data by fingerprinting the unstructed data.



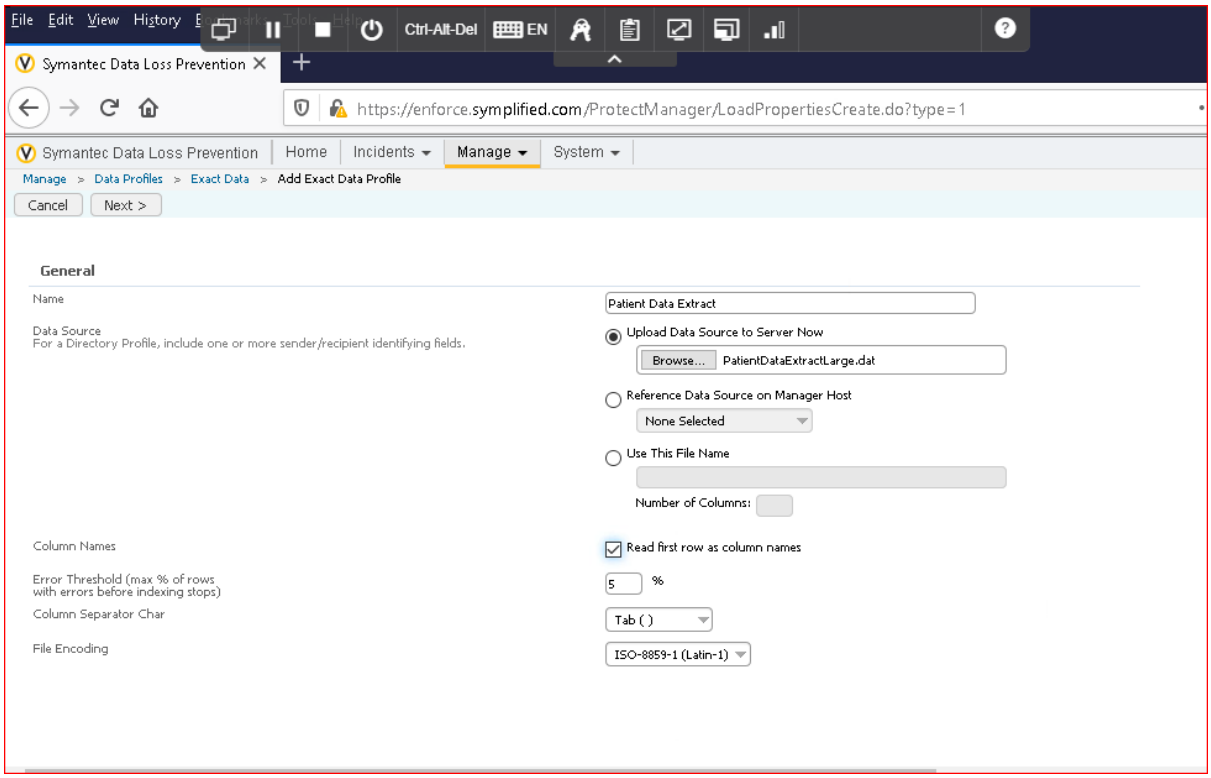
Below the status indicates that the policy is in active state and running

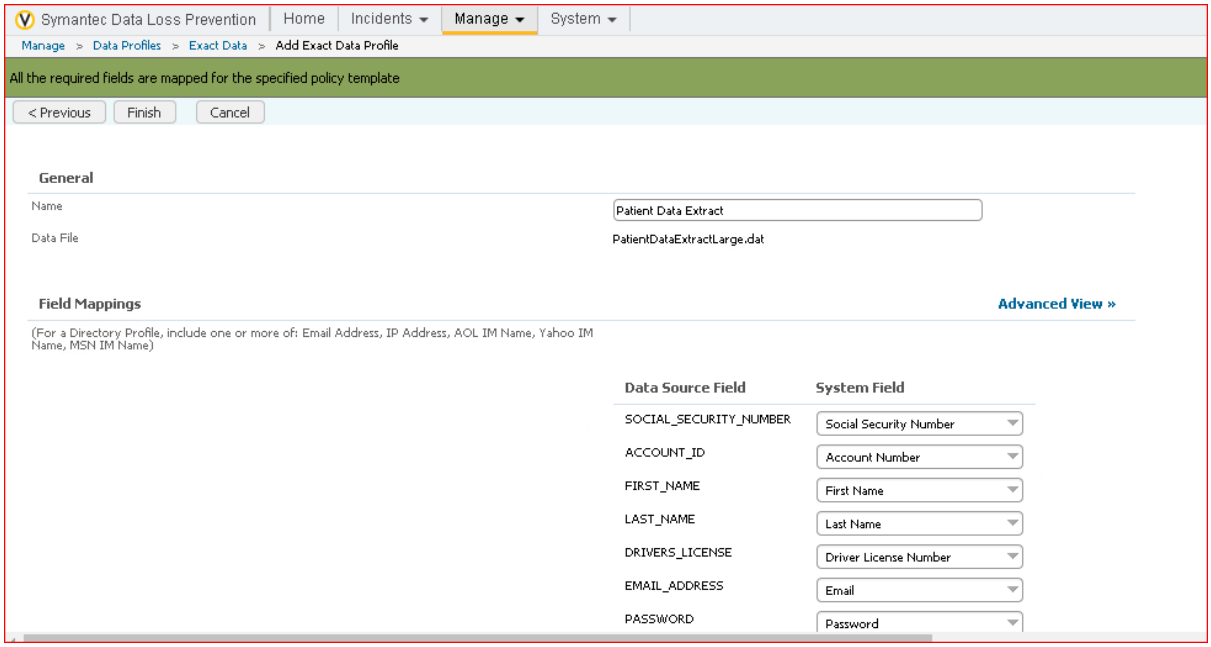
Vinay Kumar Reddy Donda dondavinayreddy@gmail.com

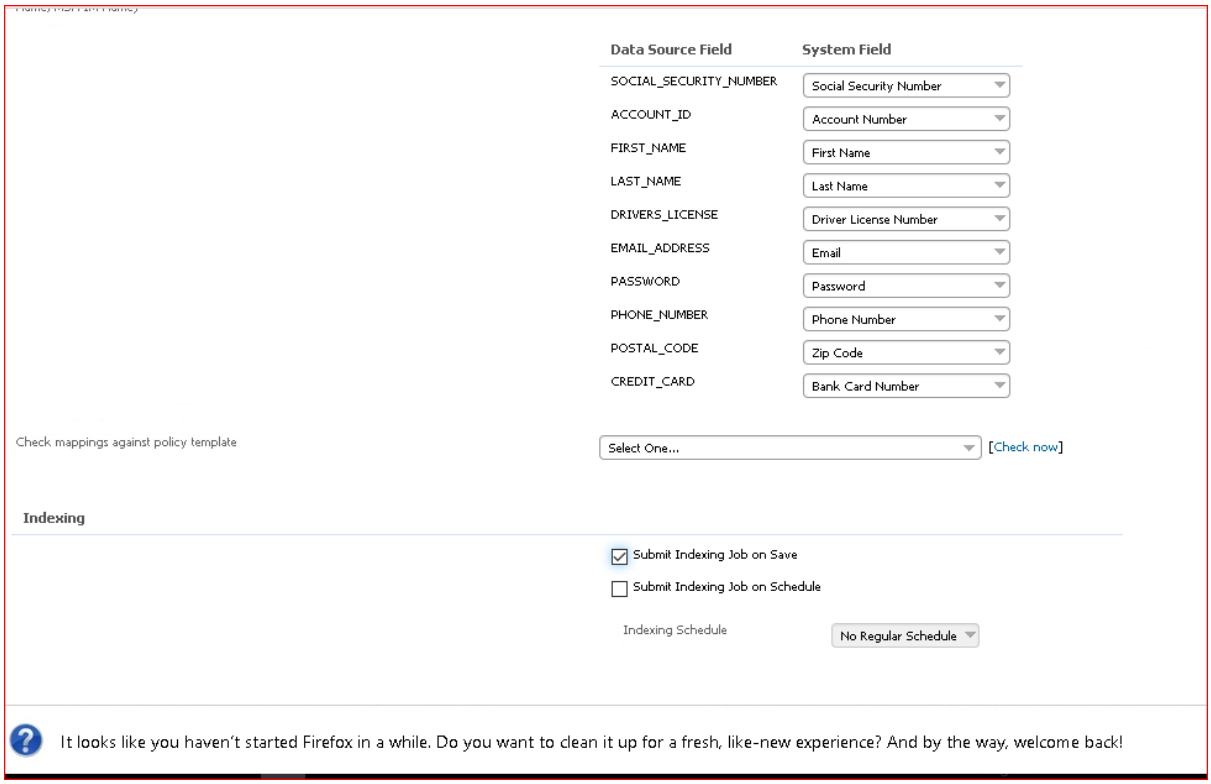
Exercise 4:

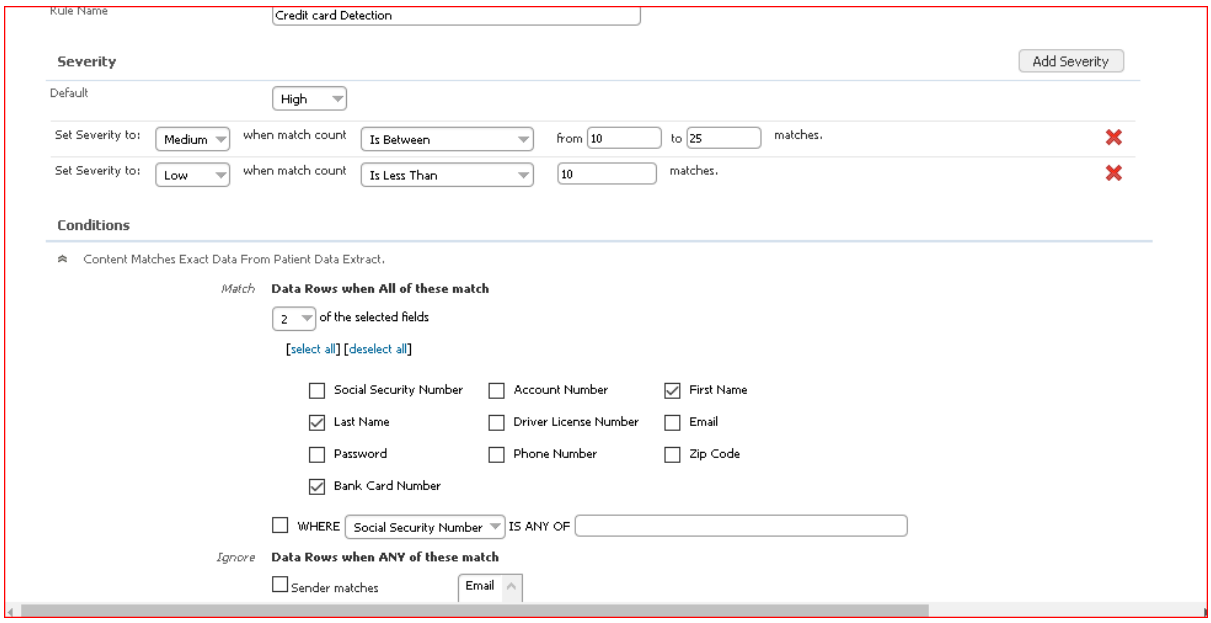
Configuring the policy for PCI compliance.

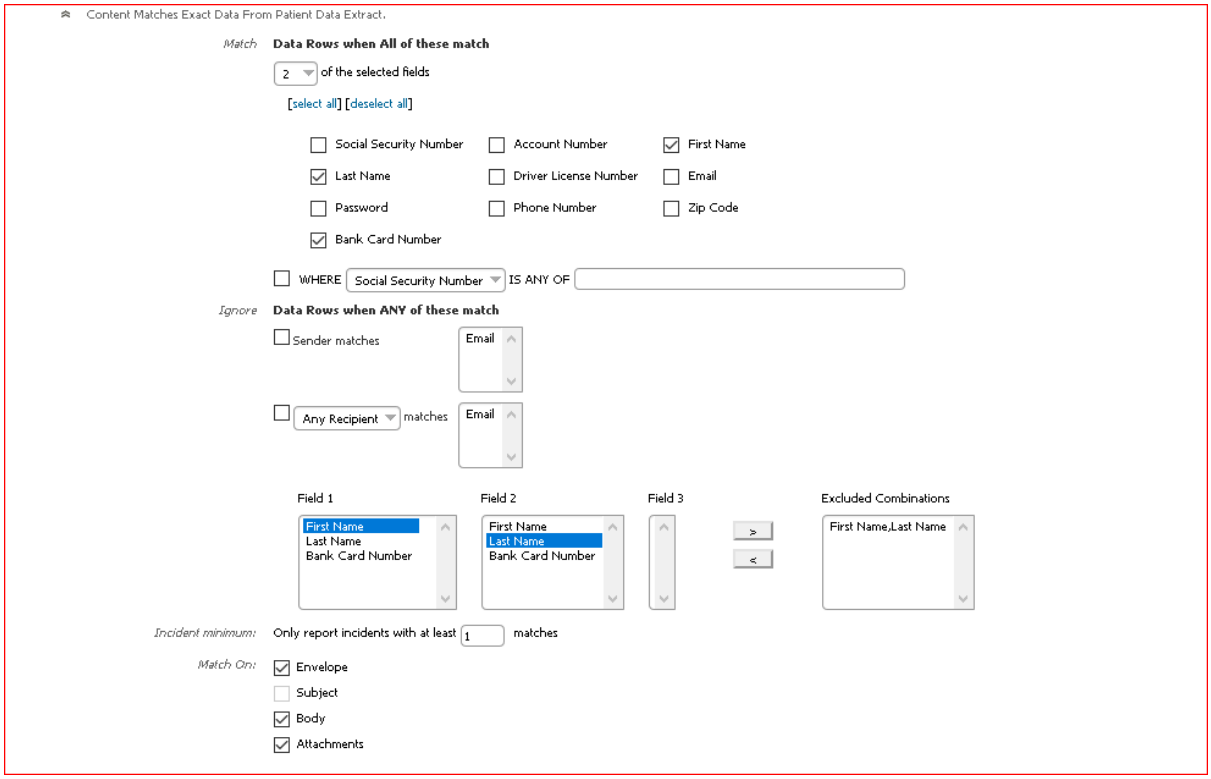
Senstive data like credit card information will be stored in the database however it is encrypted but some of the inside employees can see the unencrypted data so they can leak the information as well. The main precaution we should take is we should use the exact data match (EDM) which is done by fingerprinting the structured data. So, whenever the data is transmitted over the network EDM should identify that and for information not getting leaked we add the policies.

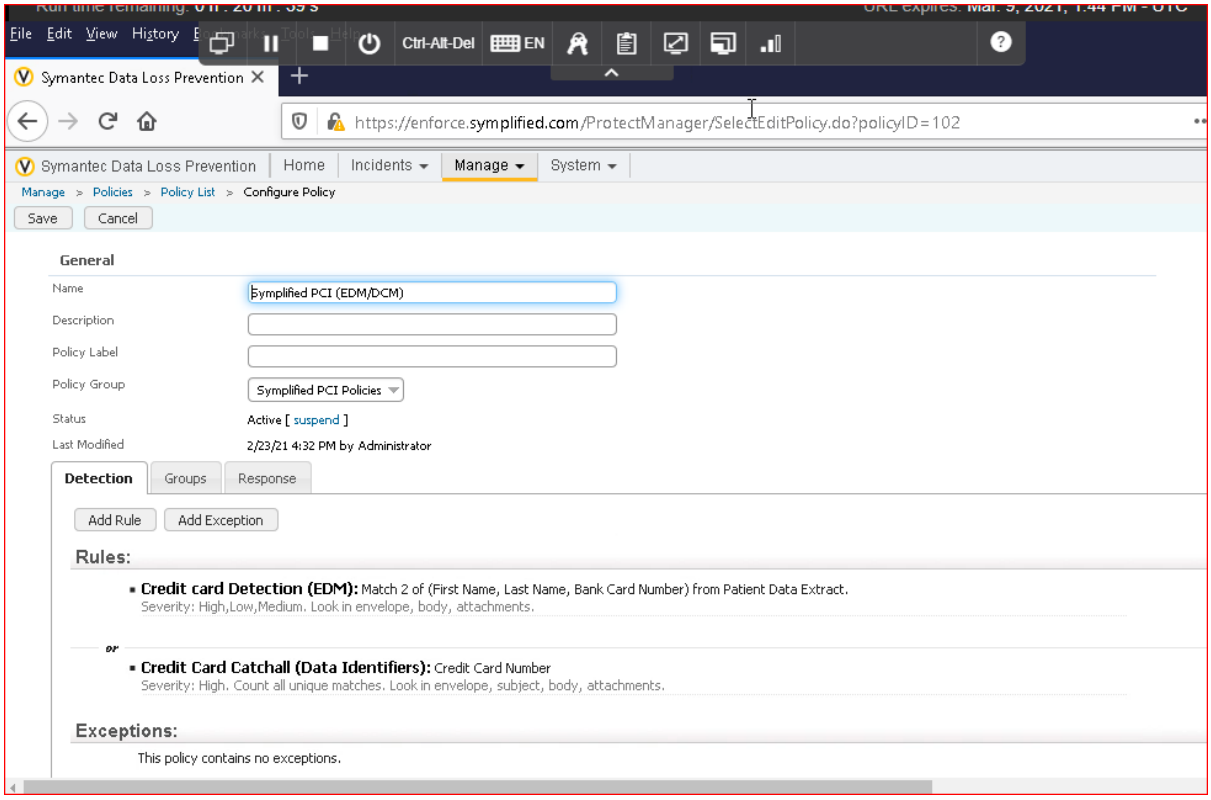




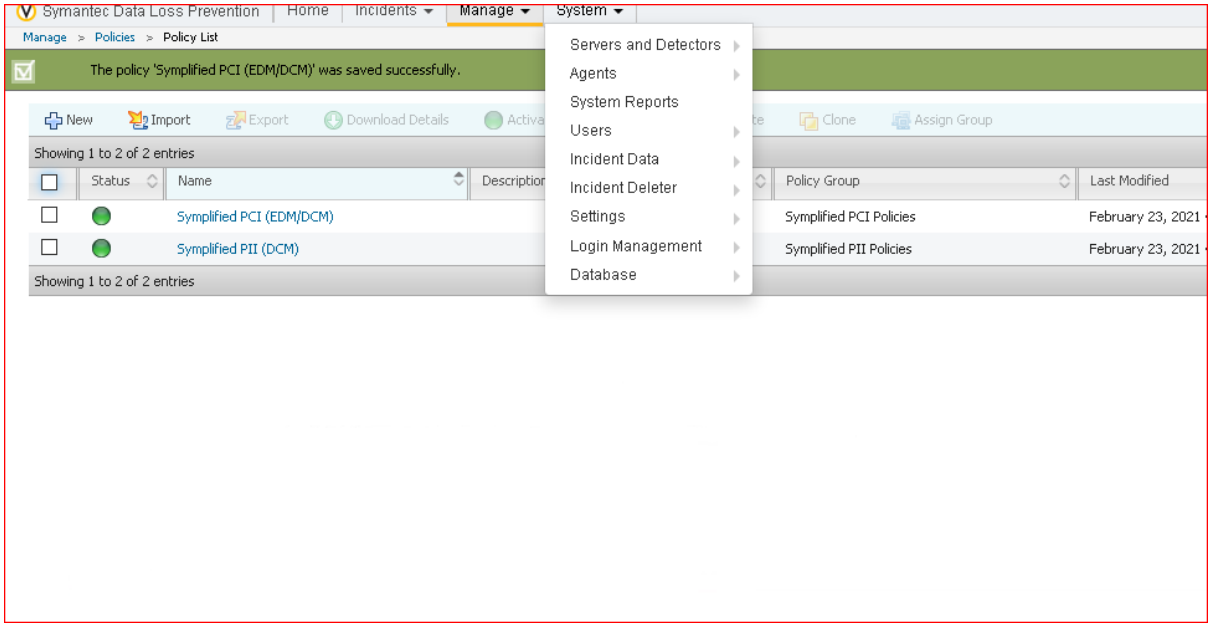

Data Source Field
System Field
SOCIAL_SECURITY_NUMBER
Social Security Number
ACCOUNT_ID
Account Number
FIRST_NAME
First Name
LAST_NAME
Last Name
DRIVERS_LICENSE
Driver License Number
EMAIL_ADDRESS
Email
PASSWORD
Password
PHONE_NUMBER
Phone Number
POSTAL_CODE
Zip Code
CREDIT_CARD
Bank Card Number
Check mappings against policy template
Select One...
[Check now]
Indexing
Submit Indexing Job on Save
Submit Indexing Job on Schedule
Indexing Schedule
No Regular Schedule
It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!


Rule Name
Credit card Detection
Severity
Add Severity
Default
High
Set Severity to:
Medium
when match count
Is Between
from 10
to 25
matches.
Set Severity to:
Low
when match count
Is Less Than
10
matches.
Conditions
Content Matches Exact Data From Patient Data Extract.
Match
Data Rows when All of these match
2
of the selected fields
[select all] [deselect all]
Social Security Number
Account Number
First Name
Last Name
Driver License Number
Email
Password
Phone Number
Zip Code
Bank Card Number
WHERE
Social Security Number
IS ANY OF
Ignore
Data Rows when ANY of these match
Sender matches
Email


Content Matches Exact Data From Patient Data Extract.
Match
Data Rows when All of these match
2 of the selected fields
[select all] [deselect all]
Social Security Number
Account Number
First Name
Last Name
Driver License Number
Email
Password
Phone Number
Zip Code
Bank Card Number
WHERE Social Security Number IS ANY OF
Ignore
Data Rows when ANY of these match
Sender matches
Email
Any Recipient matches
Email
Field 1
Field 2
Field 3
Excluded Combinations
First Name
Last Name
Bank Card Number
First Name
Last Name
Bank Card Number
First Name,Last Name
Incident minimum:
Only report incidents with at least 1 matches
Match On:
Envelope
Subject
Body
Attachments


File Edit View History
Ctrl-Alt-Del
EN
Symantec Data Loss Prevention
https://enforce.symplified.com/ProtectManager/SelectEditPolicy.do?policyID=102
Symantec Data Loss Prevention
Home
Incidents
Manage
System
Manage > Policies > Policy List > Configure Policy
Save
Cancel
General
Name
Symplified PCI (EDM/DCM)
Description
Policy Label
Policy Group
Symplified PCI Policies
Status
Active [suspend]
Last Modified
2/23/21 4:32 PM by Administrator
Detection
Groups
Response
Add Rule
Add Exception
Rules:
Credit card Detection (EDM): Match 2 of (First Name, Last Name, Bank Card Number) from Patient Data Extract.
Severity: High,Low,Medium. Look in envelope, body, attachments.
or
Credit Card Catchall (Data Identifiers): Credit Card Number
Severity: High. Count all unique matches. Look in envelope, subject, body, attachments.
Exceptions:
This policy contains no exceptions.

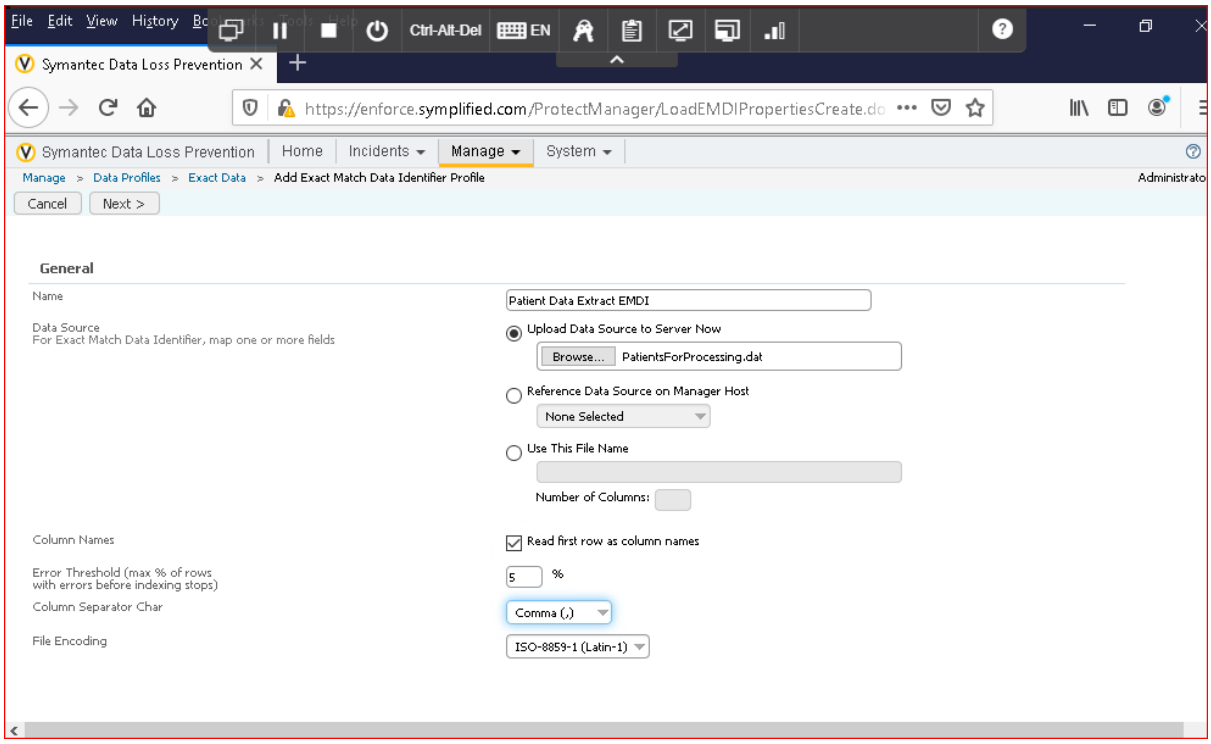
Vinay Kumar Reddy Donda dondavinayreddy@gmail.com

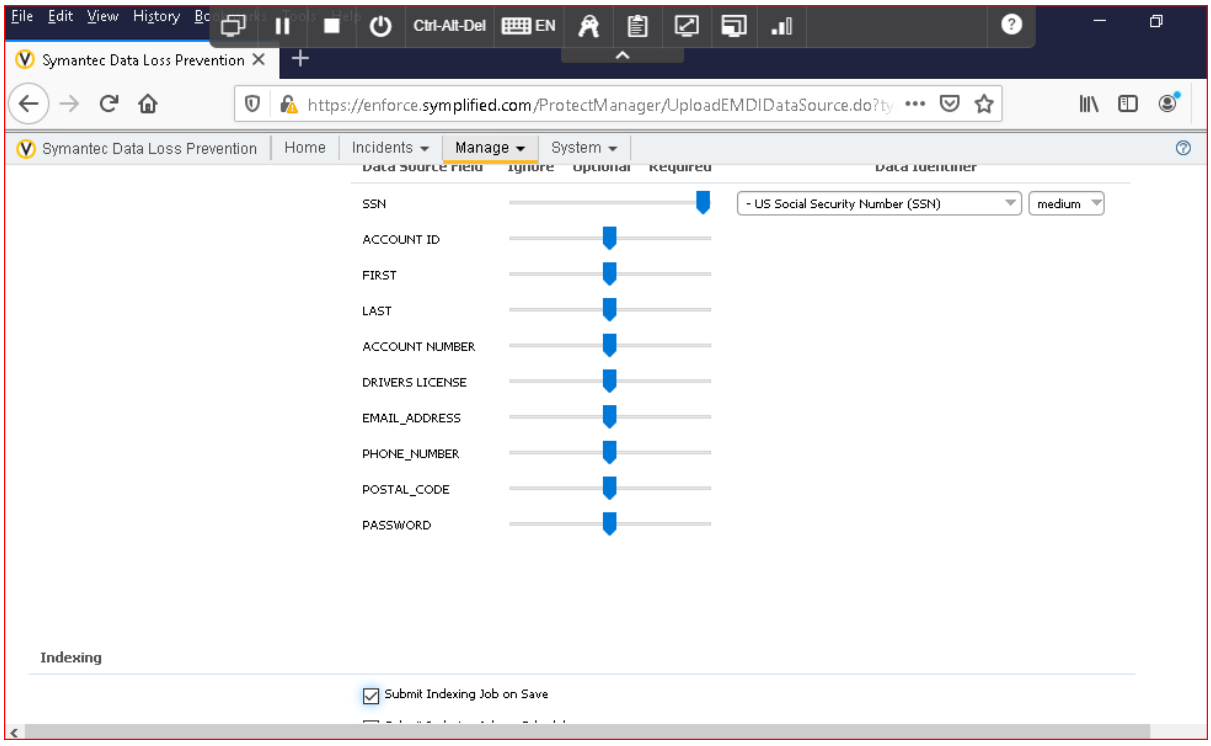


Vinay Kumar Reddy Donda dondavinayreddy@gmail.com

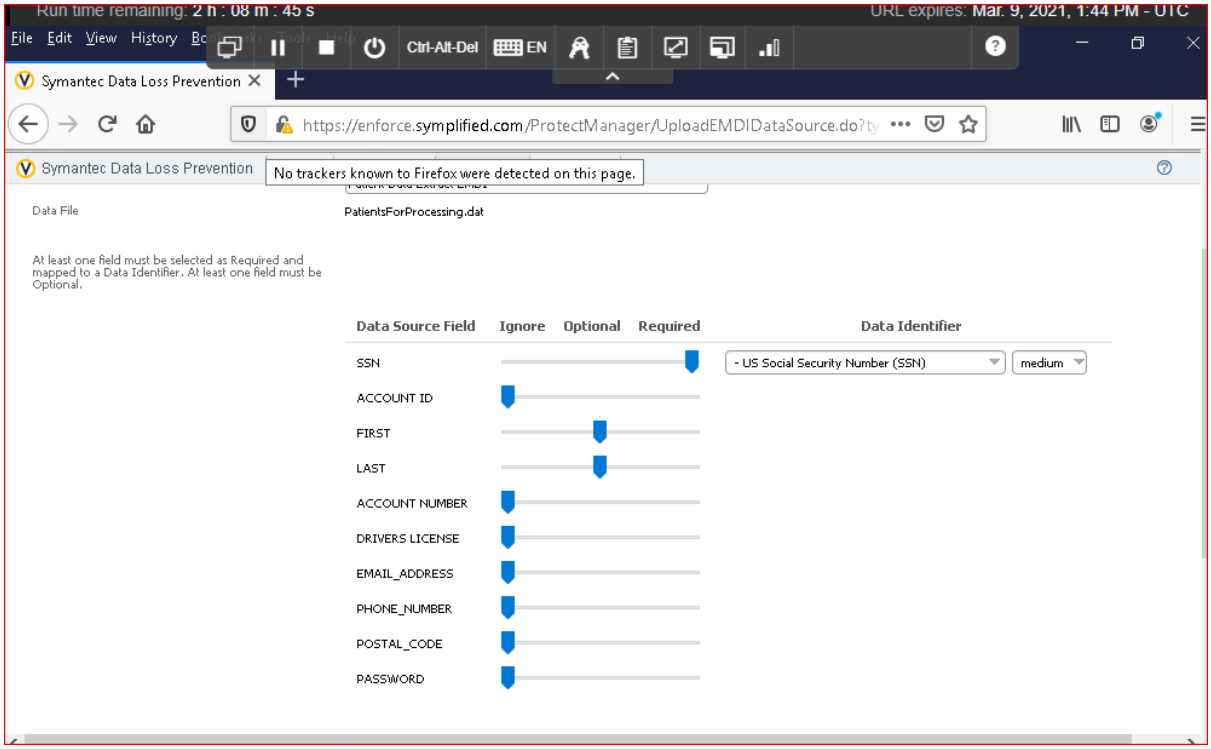
Exercise 5:

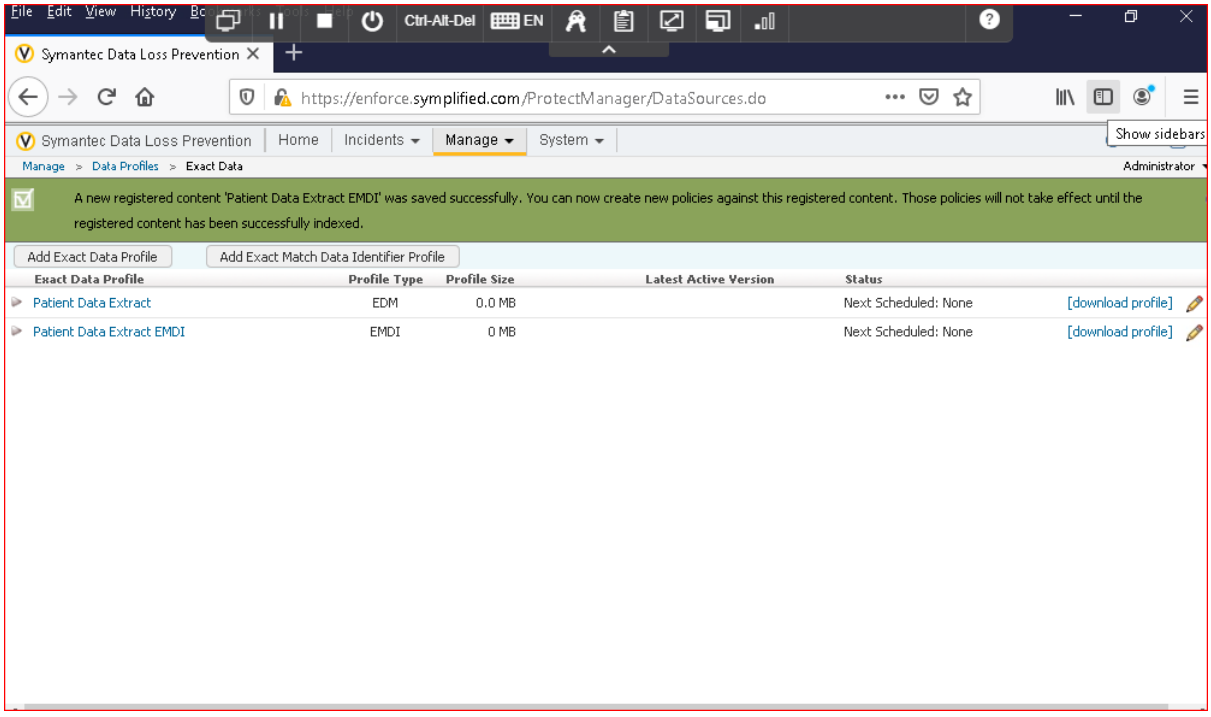
Configure and alternate policy for PII Compliance.

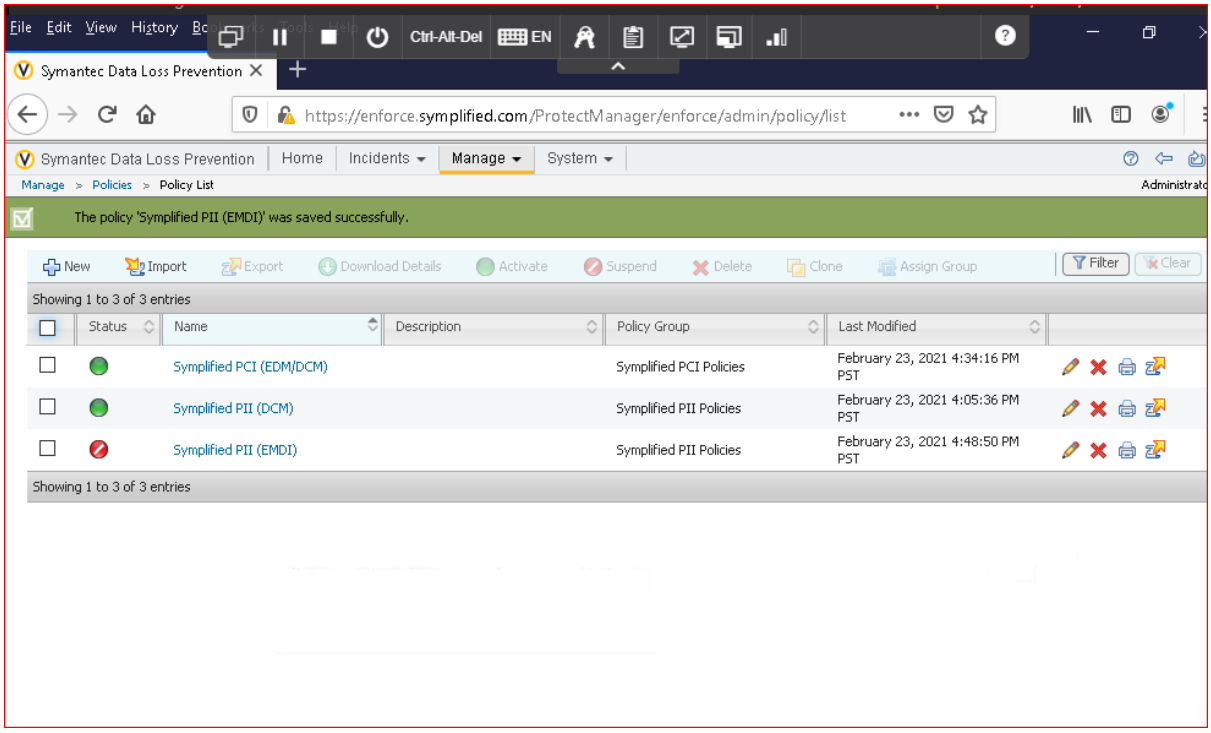




Vinay Kumar Reddy Donda dondavinayreddy@gmail.com







This indicates that added policy is not active.

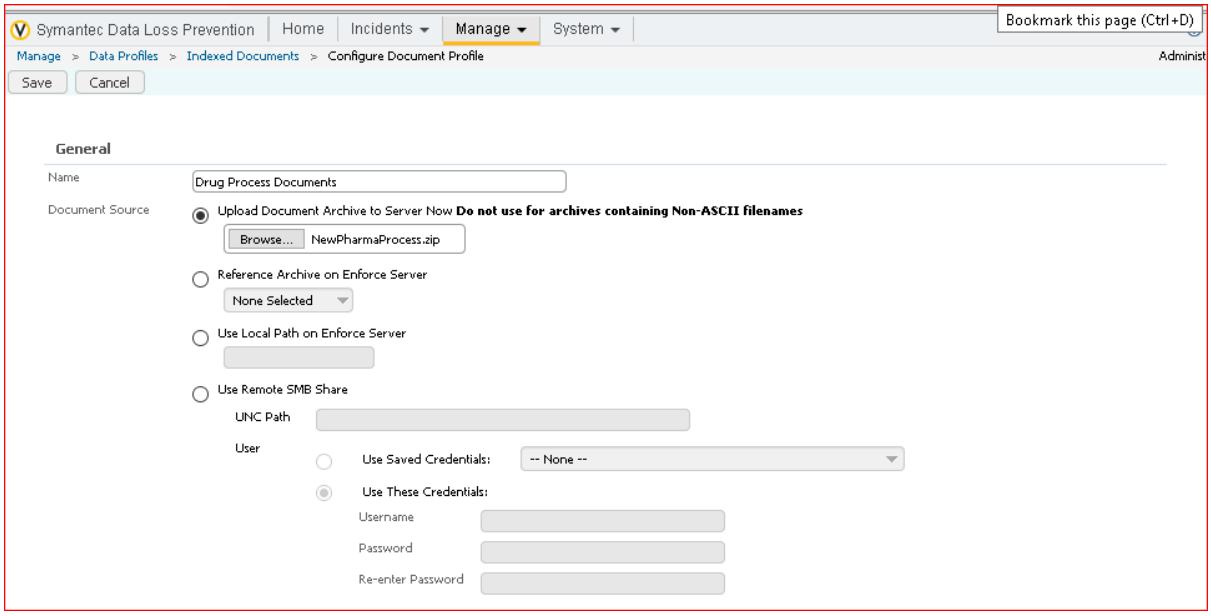
Vinay Kumar Reddy Donda dondavinayreddy@gmail.com

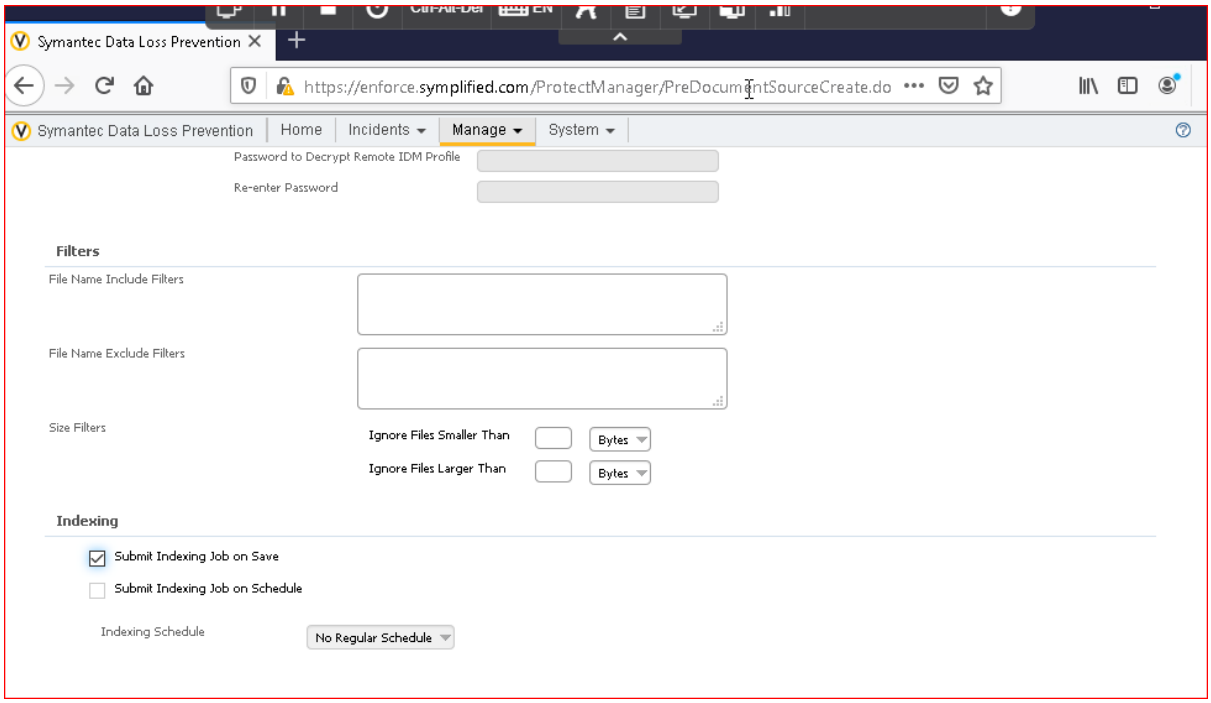
Exercise 6:

Configure a policy to protect the confidential document.

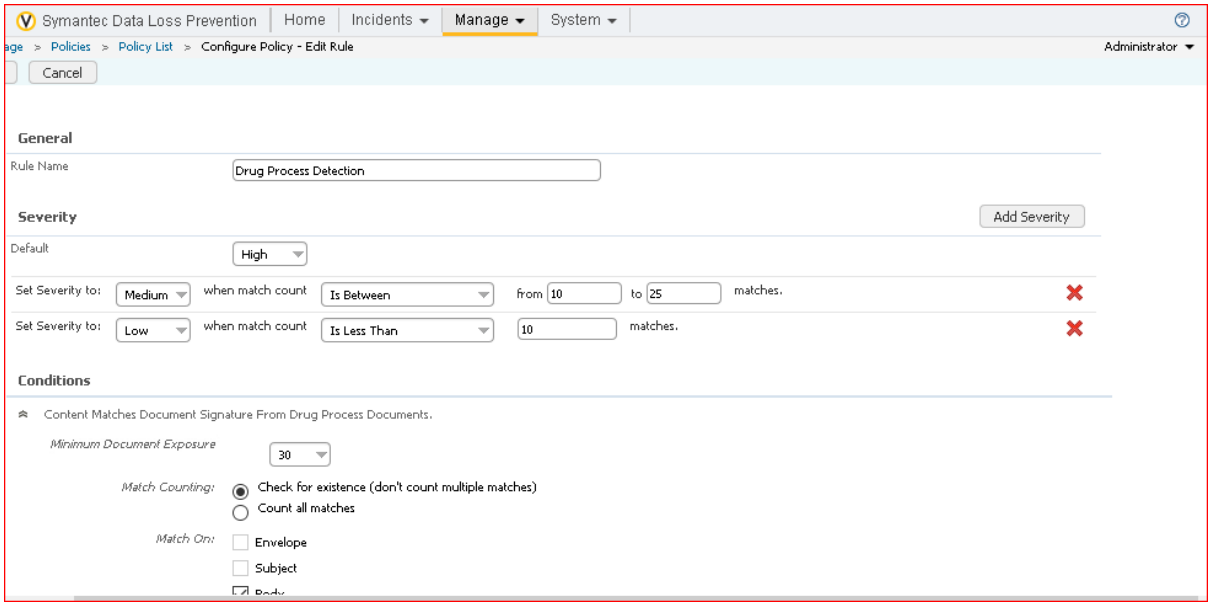
It used the INDEXED DOCUMENT MATCHING.

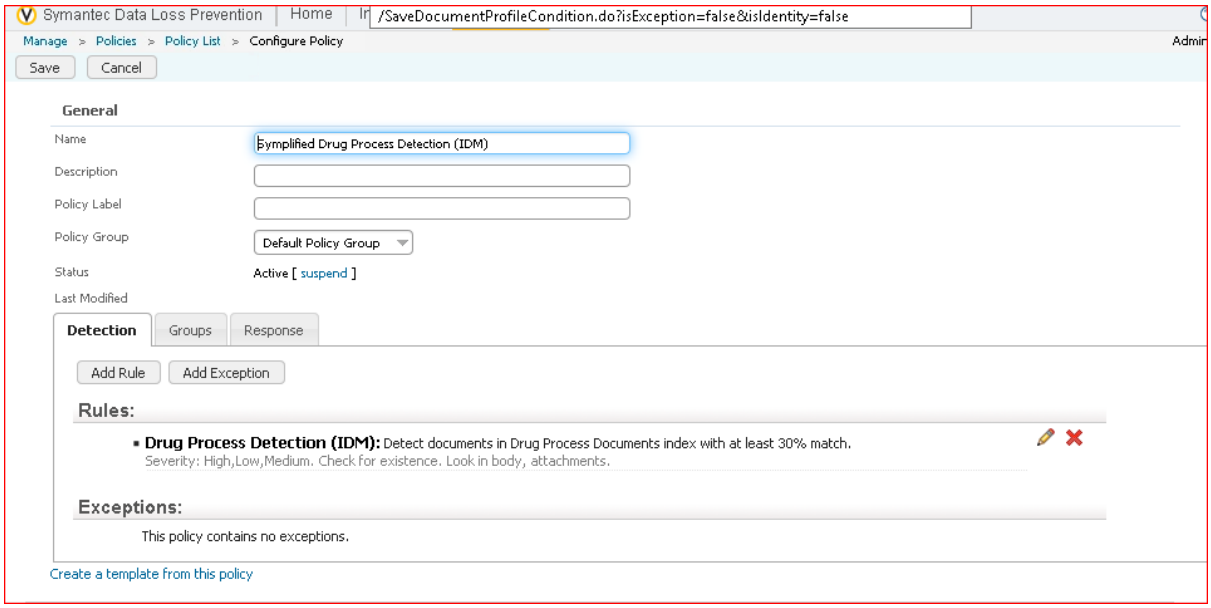
For instance, a medical company discovered the new drug and whole details were there in the pdf and the pdf should not be leaked outside especially into the competitors. For this we use the INDEXED DOCUMENT MATCHING.

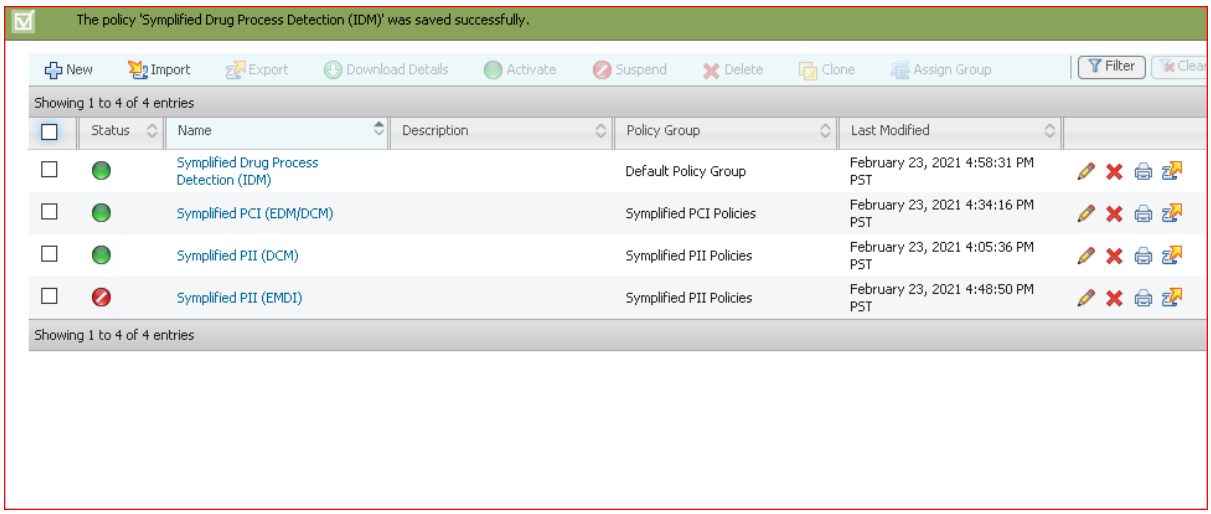




Vinay Kumar Reddy Donda dondavinayreddy@gmail.com





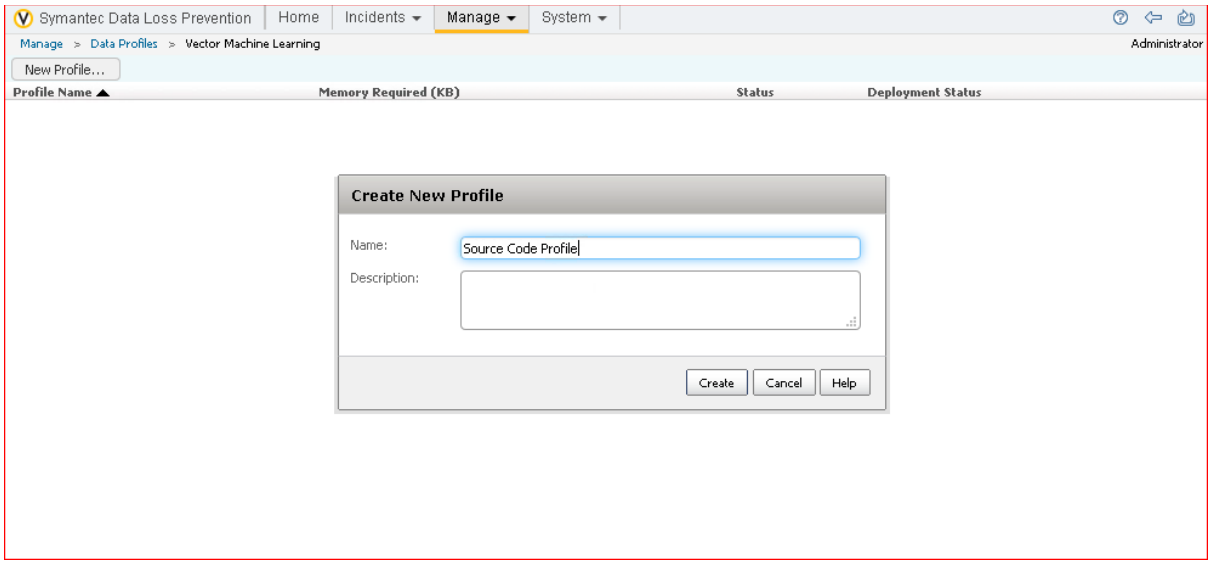


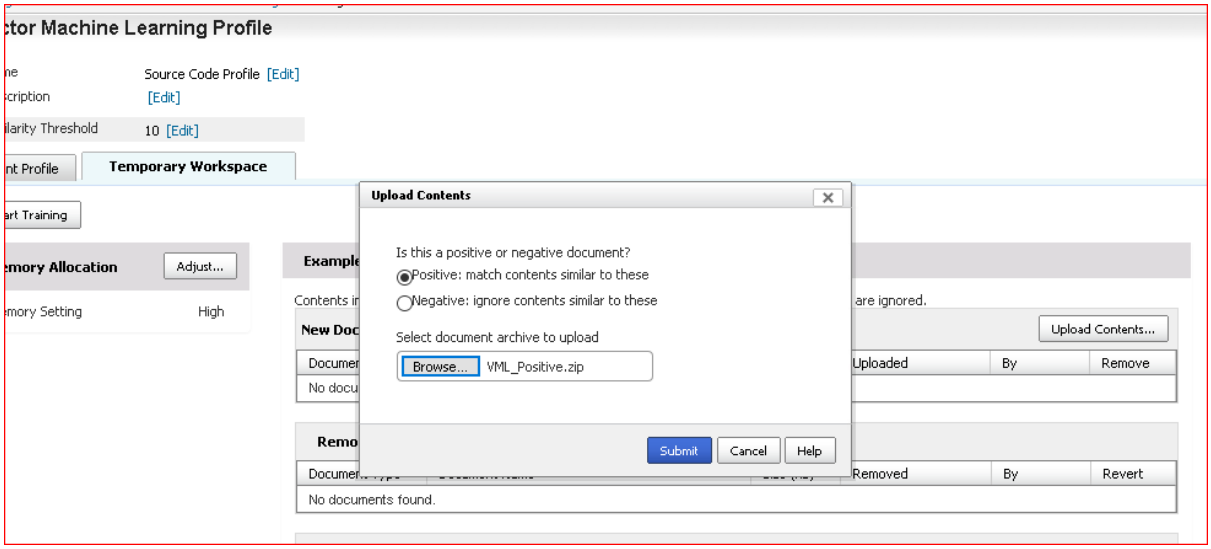
Vinay Kumar Reddy Donda dondavinayreddy@gmail.com

Exercise 7:

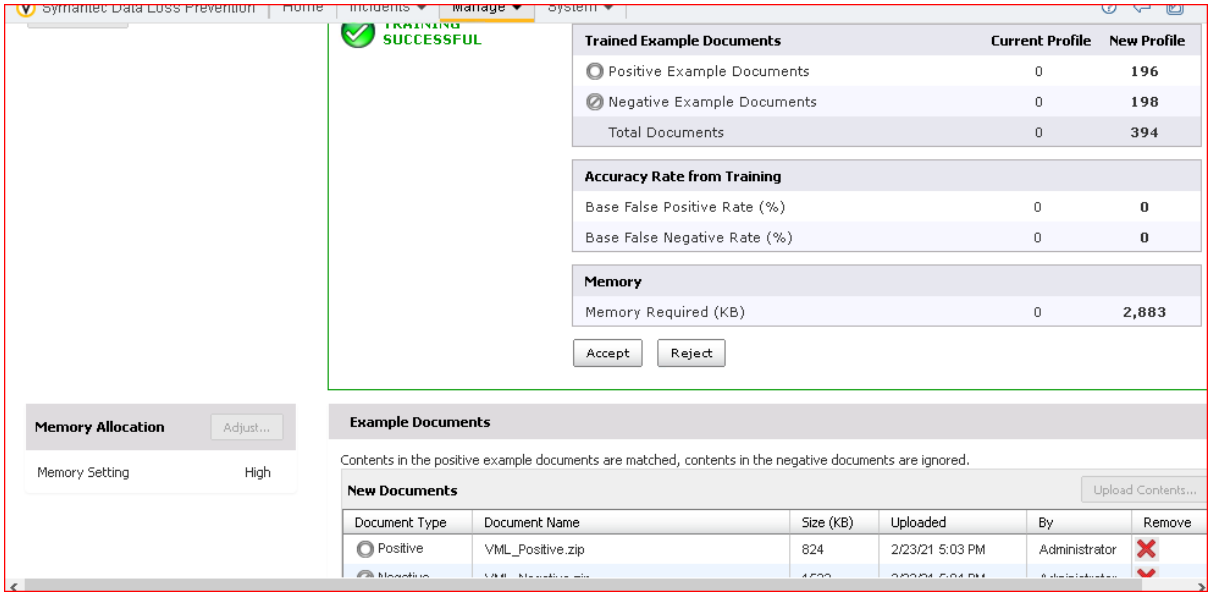
Configure the policy to protect the source code:

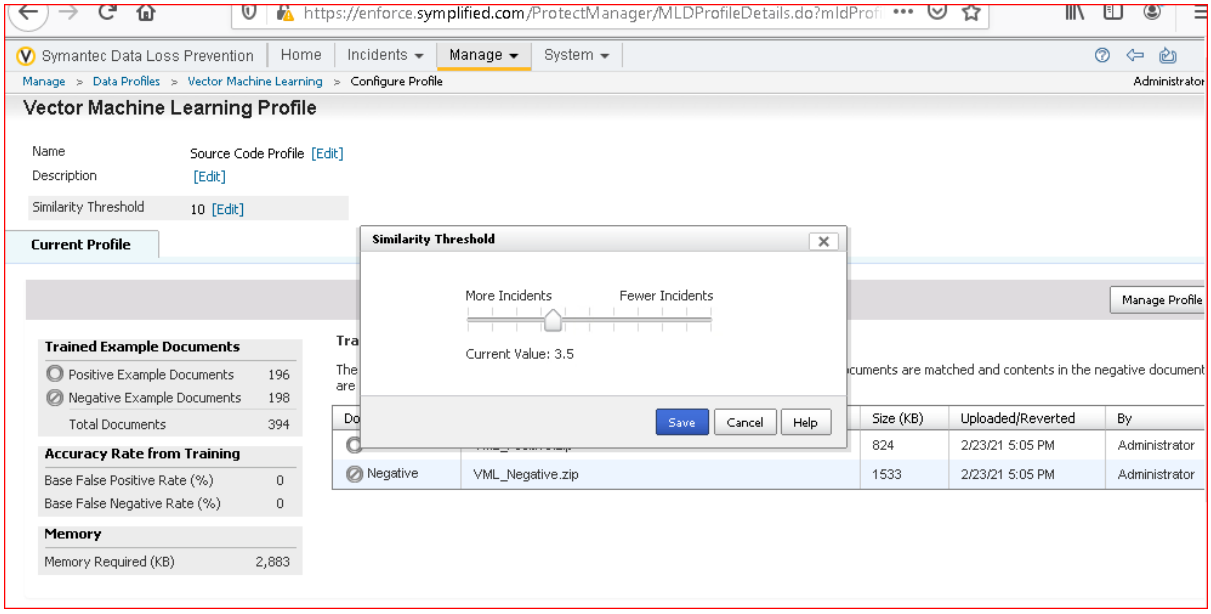
In an organization source code plays a vital and it should not be leaked as well for this we use the vector machine learning(VML) is best for finding the matches in the source code.



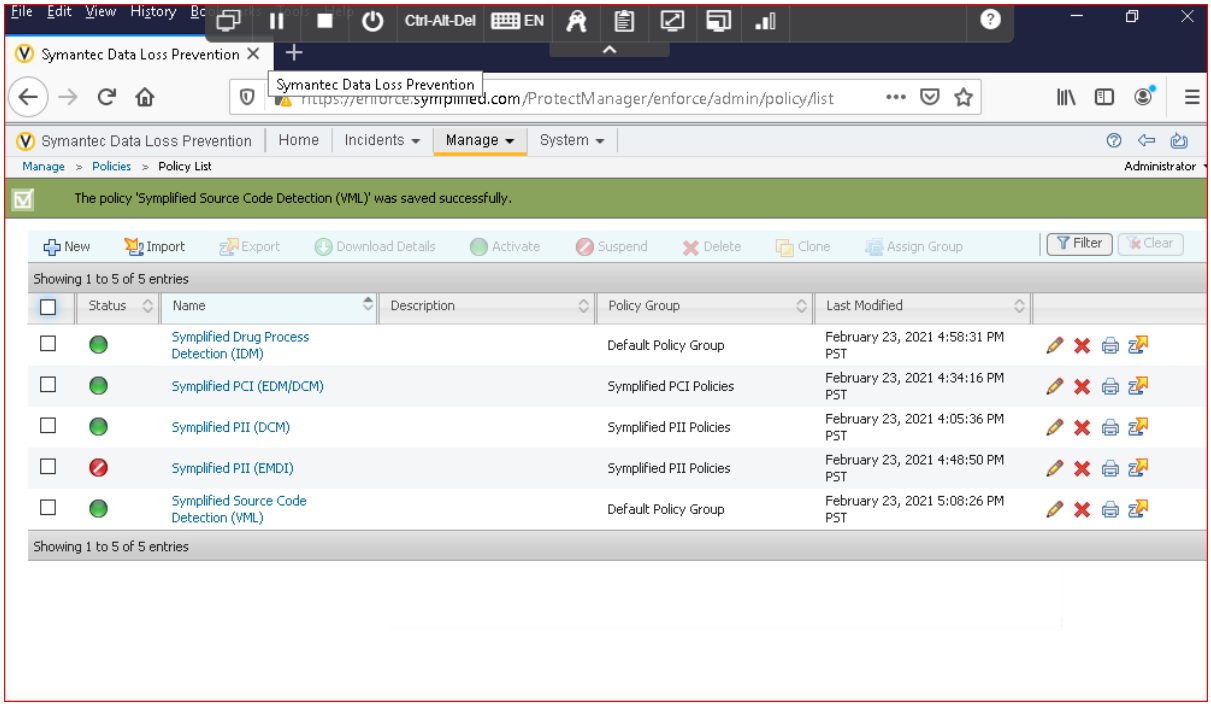


Vinay Kumar Reddy Donda dondavinayreddy@gmail.com





Vinay Kumar Reddy Donda dondavinayreddy@gmail.com



Vinay Kumar Reddy Donda dondavinayreddy@gmail.com

Exercise 8:

Configure a policy form recongintion:

Basically an organization receives or stores many forms it is not a problem if a form is empty but if there any any details in it it can cause the problem so we need to protect the data.

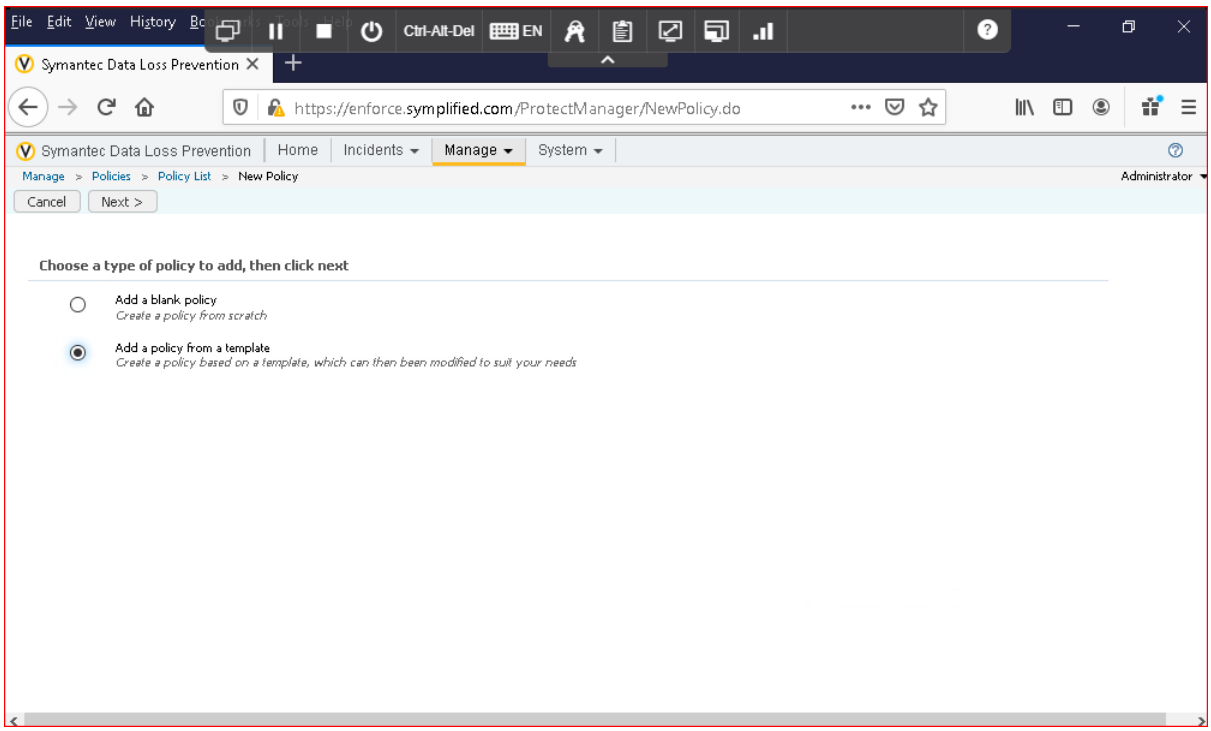
Since there is no form reconigation tab in the data profiles iam skipping the exercise 8.

Exercise 9:

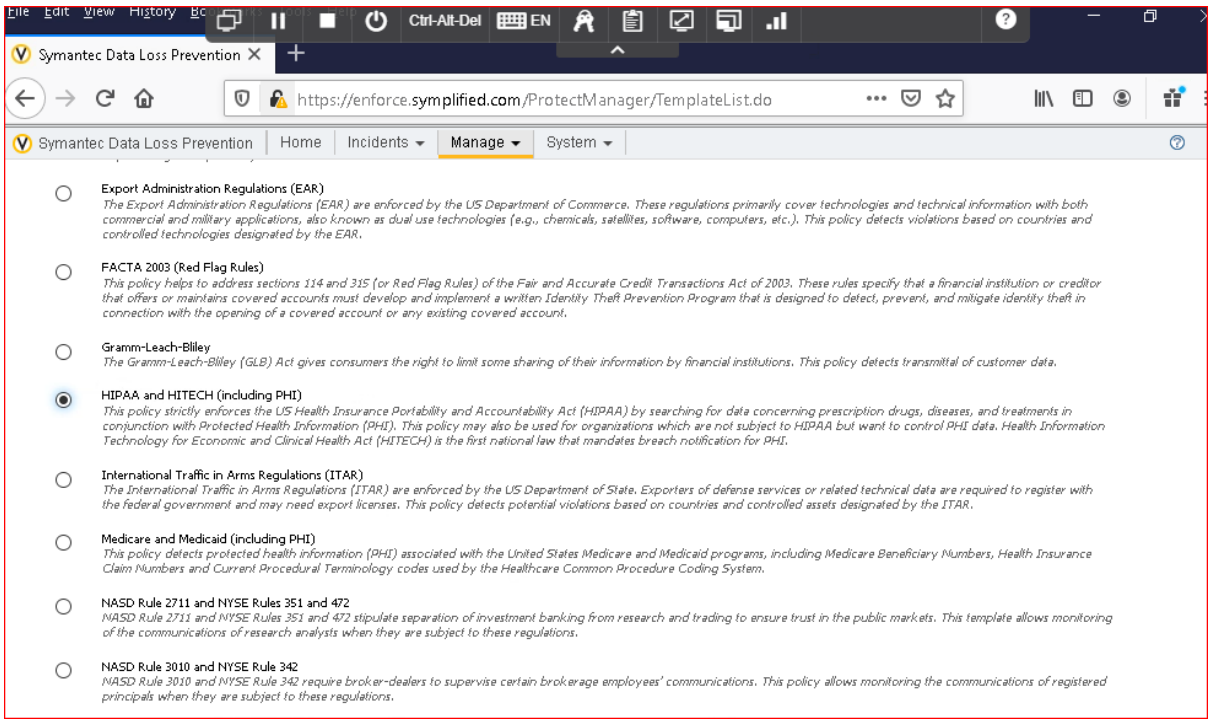
Use a template to add the DLP policy.

The templated implied that there is a policy which is already there and we just use that template and later we can modify that particular template.

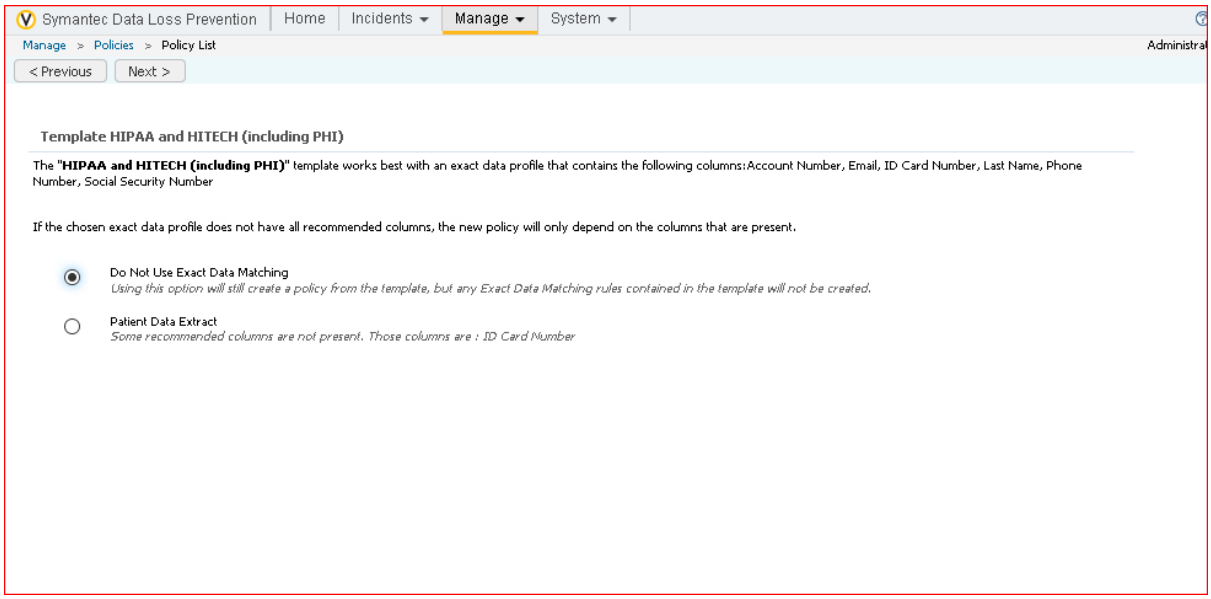
Symantec DLP ships with HIPAA template and we can use this template in order to define the policy.



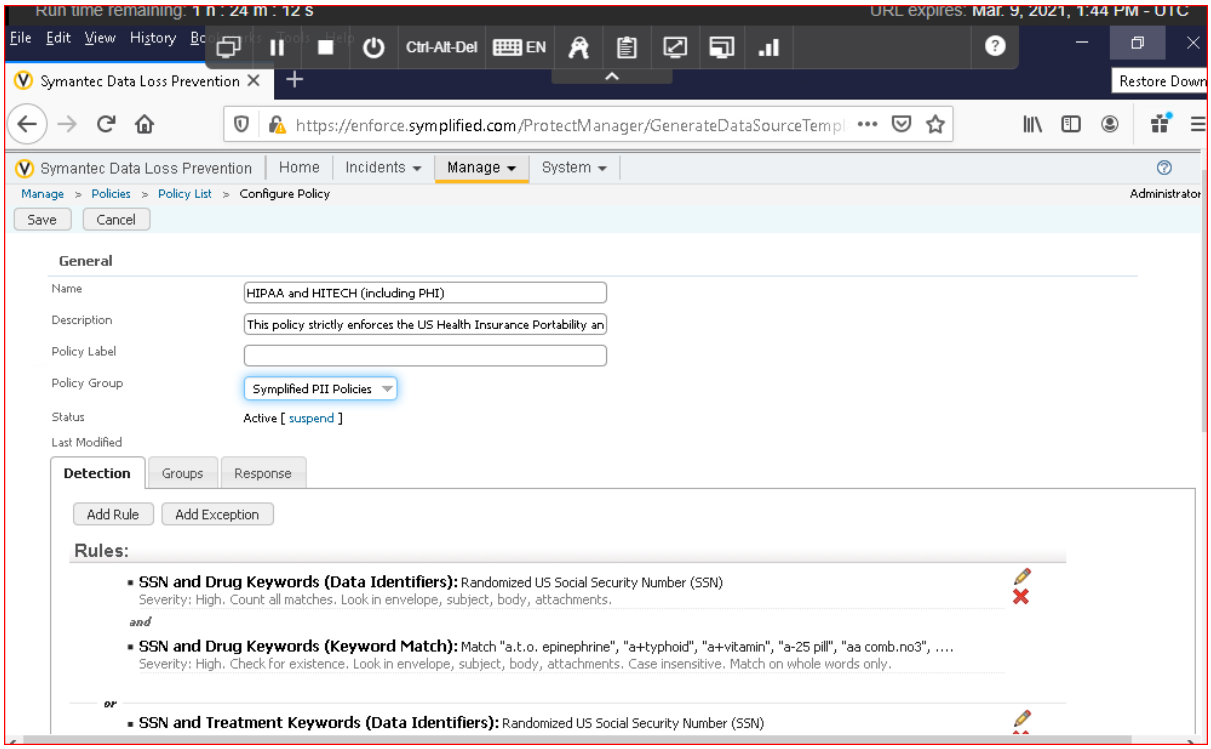
Click next



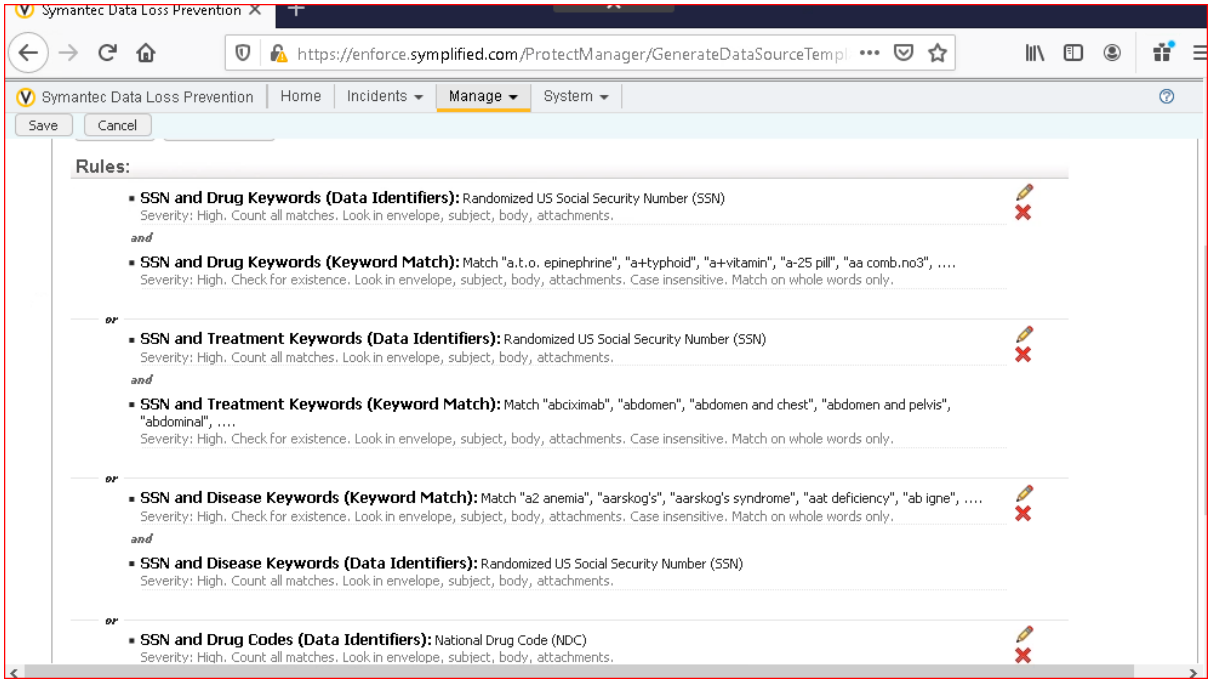
After selecting this click next



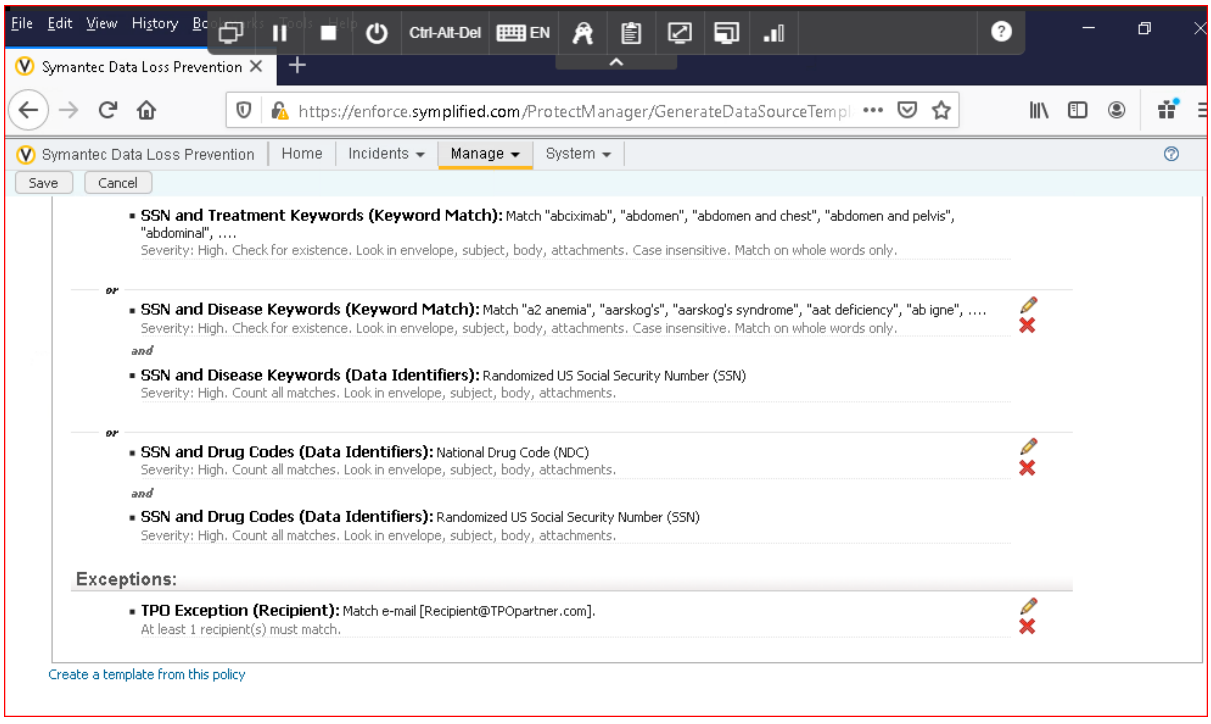
After selecting this click next



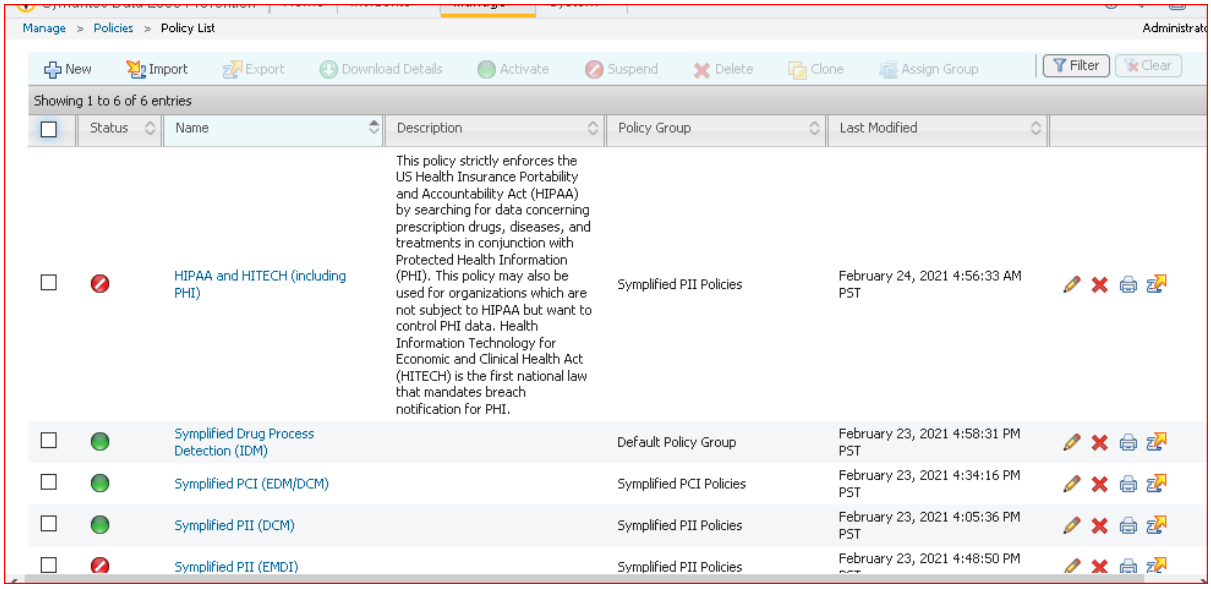
Click on save



These are the rules which are there in the template we didn't add any rules



Rules and exceptions



Since the it is not quite ready to detect the HIPAA template data we need to suspend that.

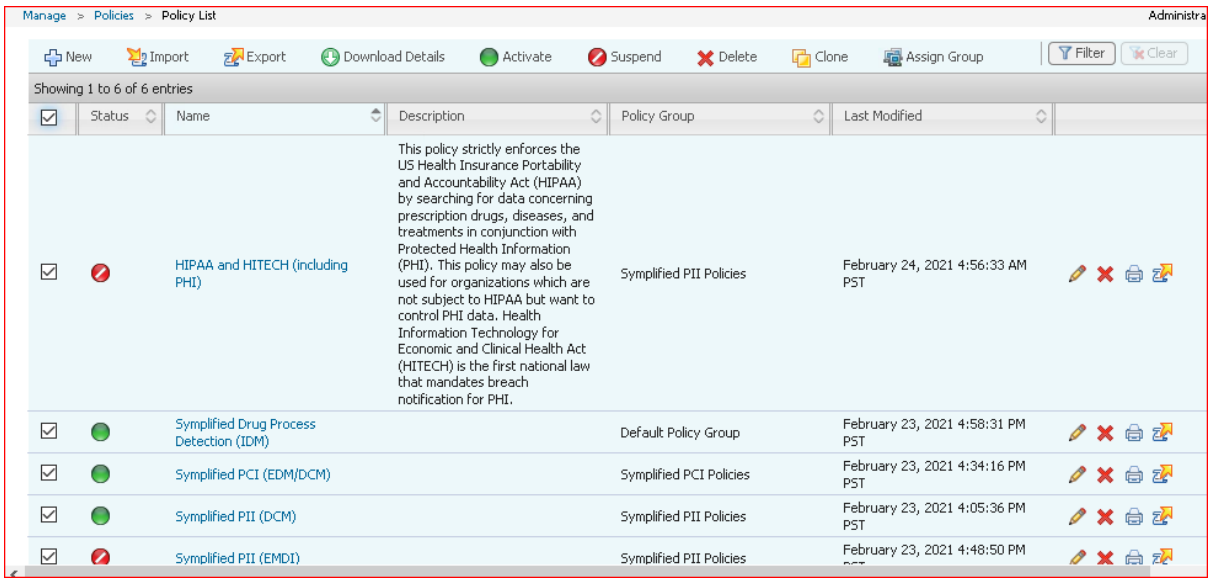
NOTE:
IN the above labs we added the rules manually but we can simply use the templates and we can modify them .

Exercise 10:

Export policies for use at the DR Site

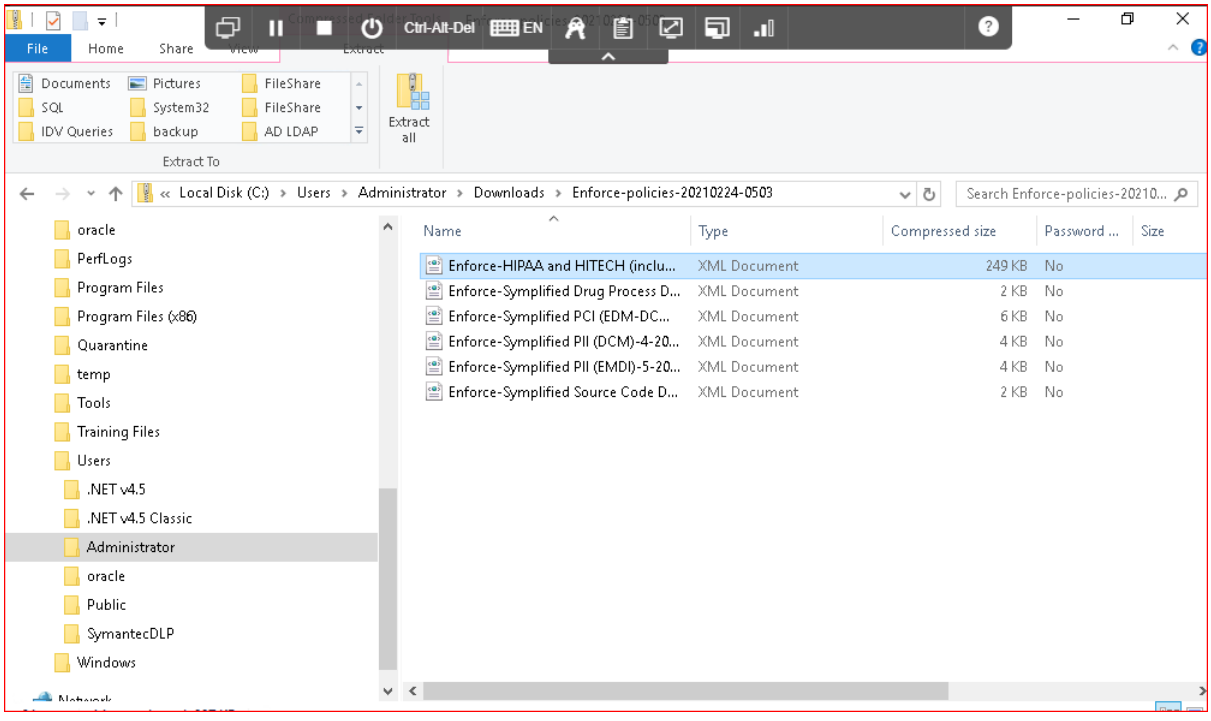
DR – Disaster Recovery.

If anything goes wrong there will be huge loss to the data and the policies as well. So we need to export the existing policies just in case if the recovery of the existing policies is needed.

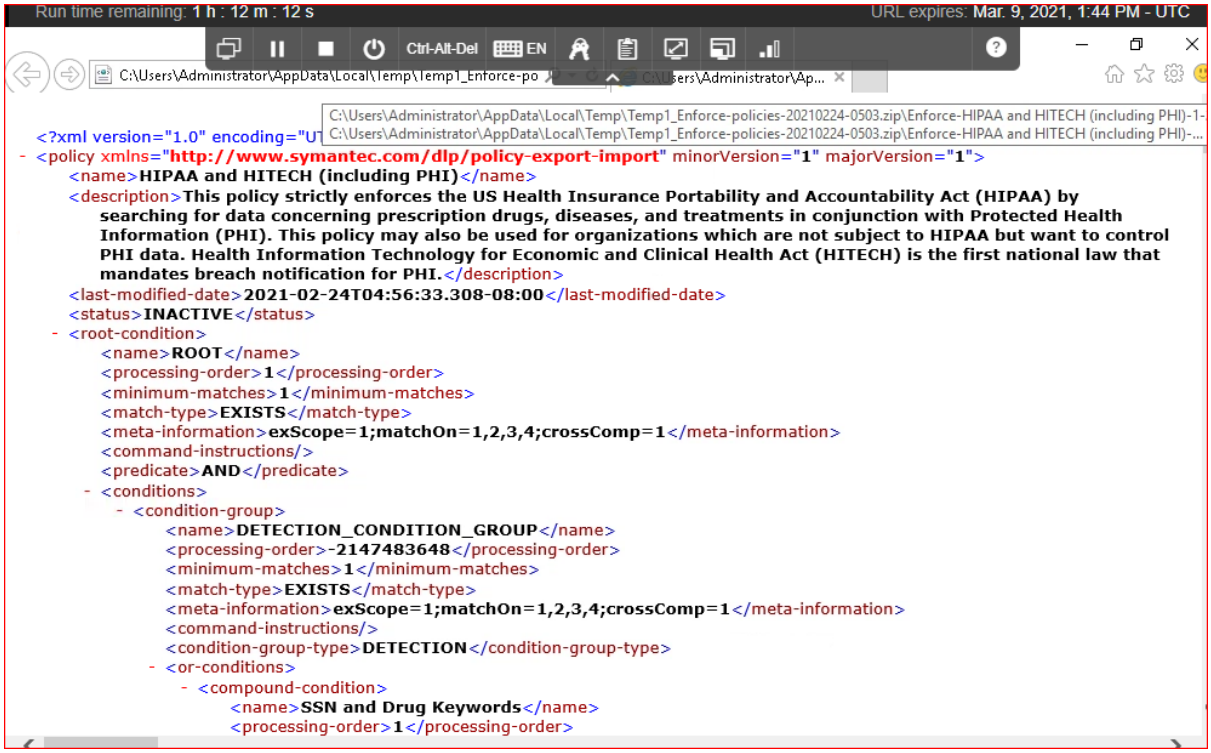


Exporting all existing policies first we need to select all and should export that I mean click on export next to import on the console.

We get a pop up window and should select for save option.



Should follow the above path for exported documents.



Here is the xml document.

Exercise 11:

Configure the optical character reconigantion.

OCR basically extracts the text from the supported image file and send this for the analysis whether if there any policy violations.

Since there is no OCR engine configuration option iam skipping this exercise.

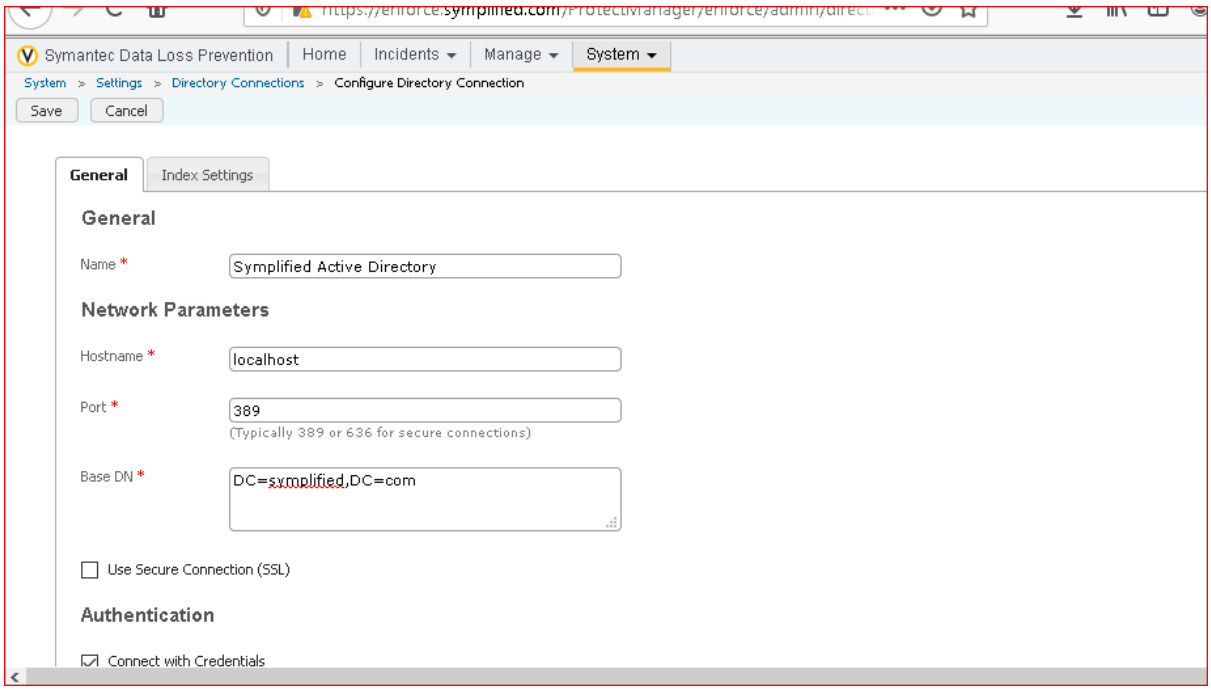
Vinay Kumar Reddy Donda dondavinayreddy@gmail.com

Locating the confidential data stored on the premises and on the cloud.

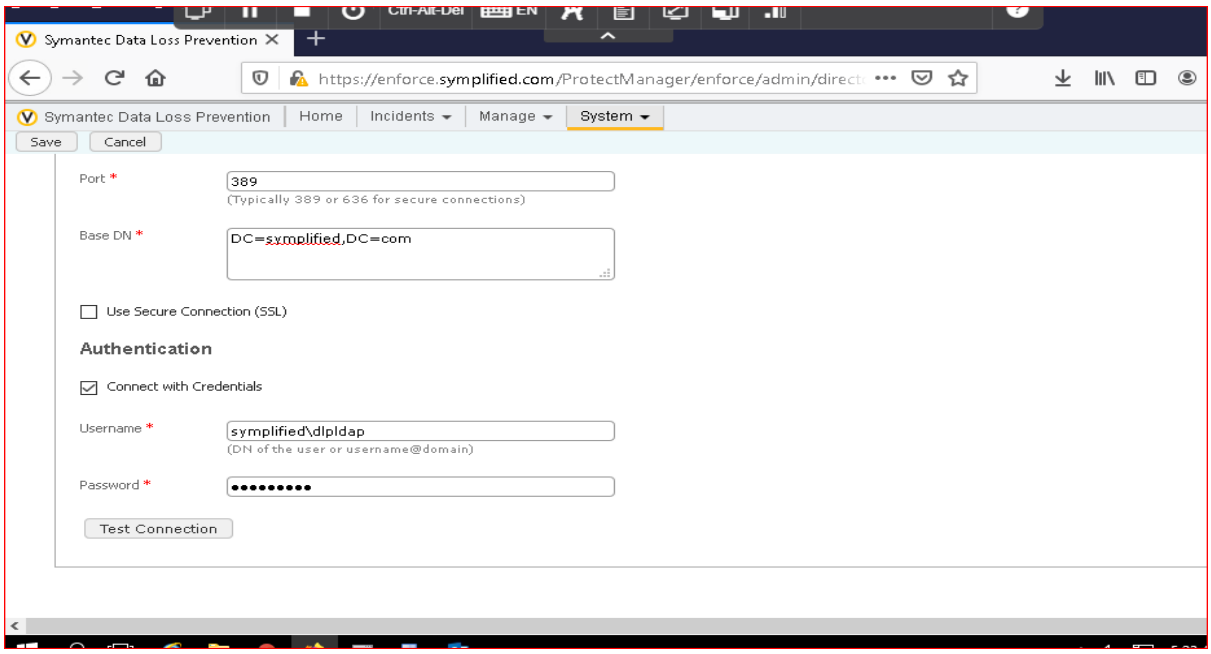
Exercise 1:

Run a Content Enumeration scan:

In an organization there will be many huge data sharing within the internal network and most of the times the data wont be well documented and it is difficult to know where this shares reside so this scan can possibly locate the shares on the network.



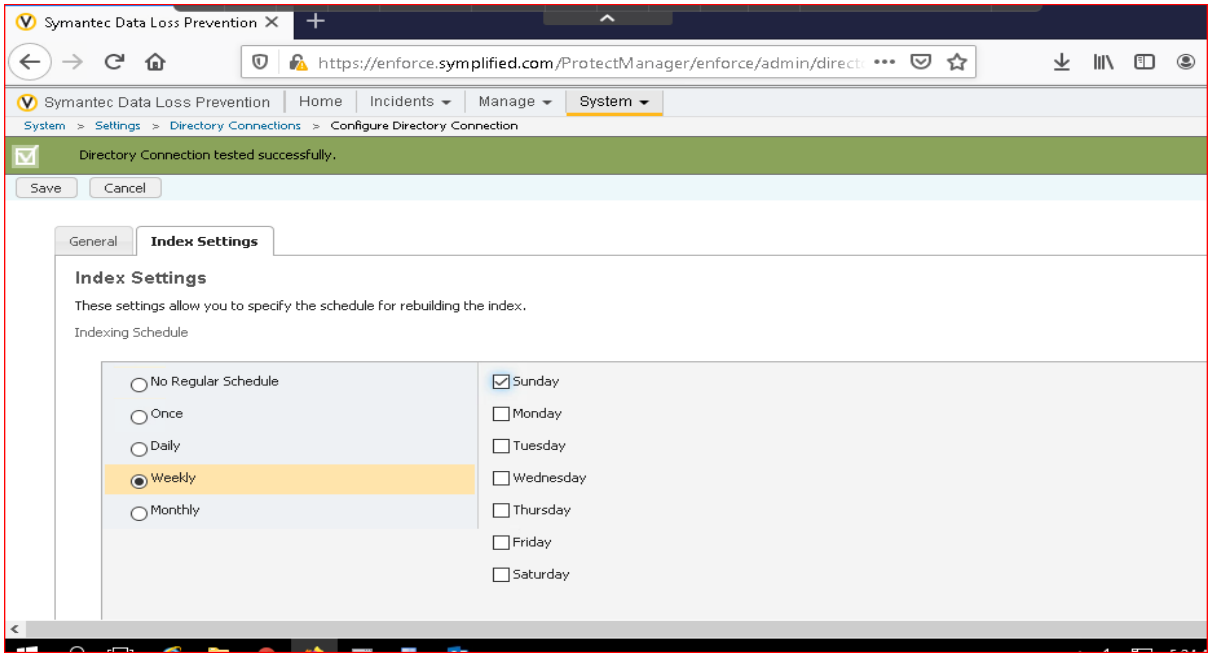
Configuring the connection to simplified active directory. Before doing enumerated scan we need to do this steps



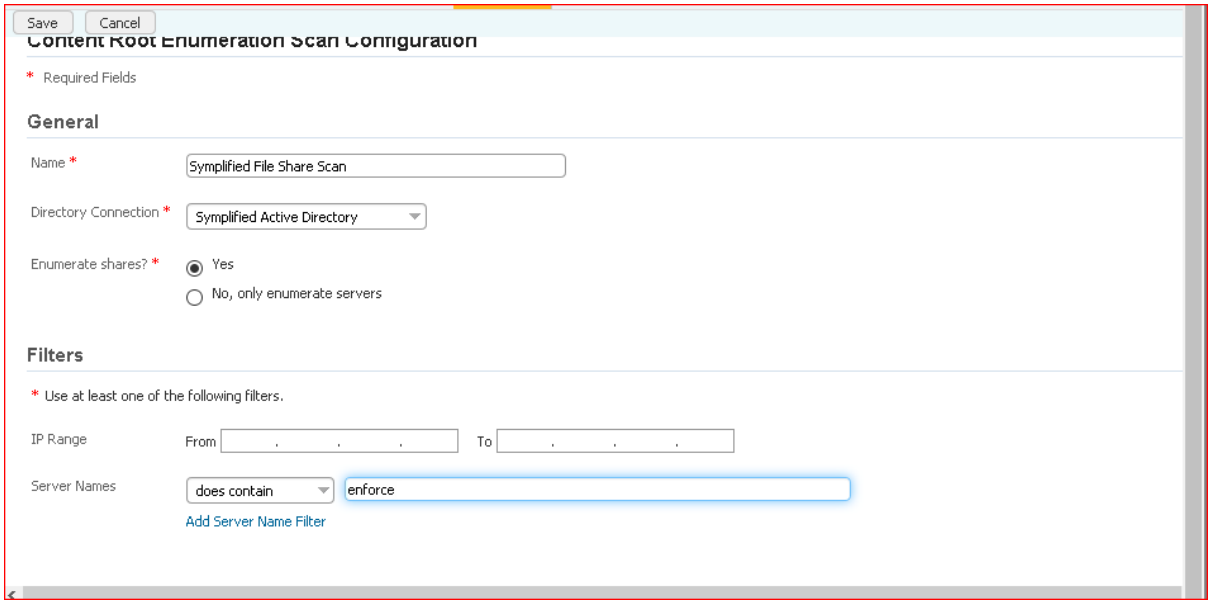
Vinay Kumar Reddy Donda dondavinayreddy@gmail.com

Configuring the connection to simplified active directory.

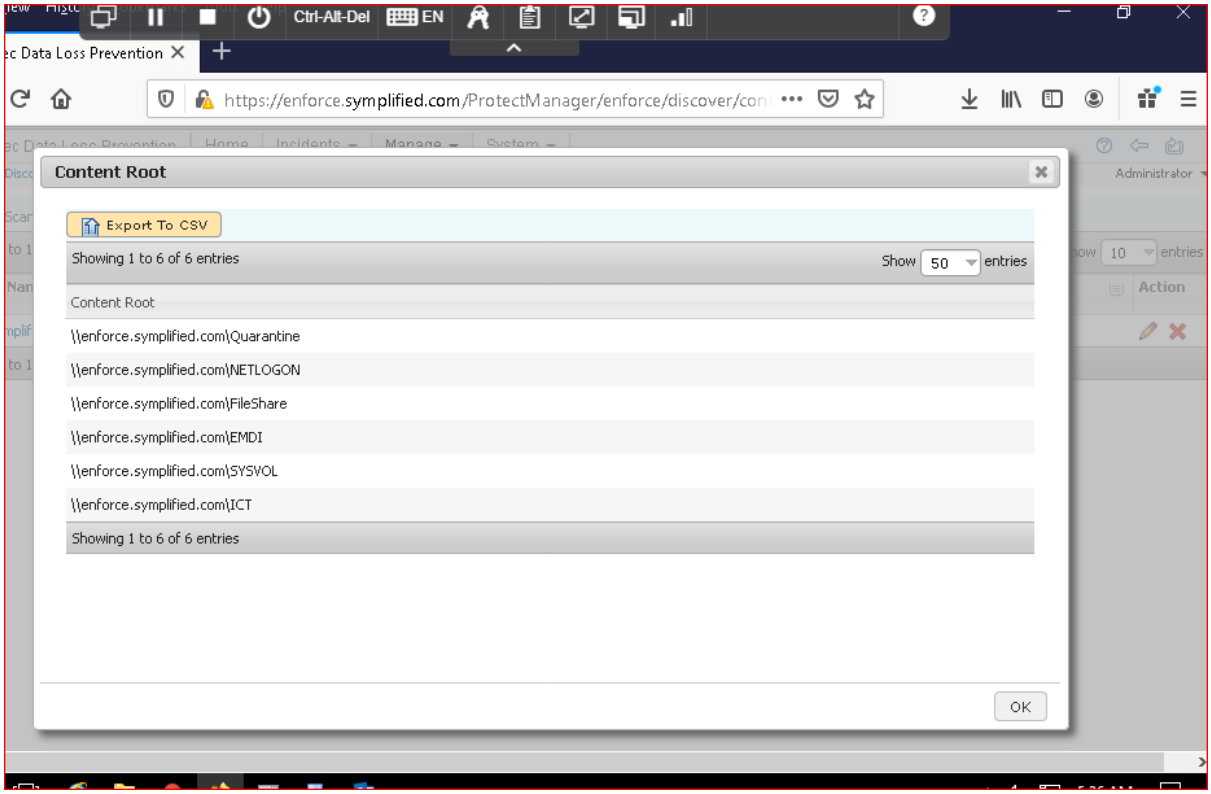
Training! Is the password



Configuring the connection to simplified active directory.s



Configuring the content root enumeration scan.



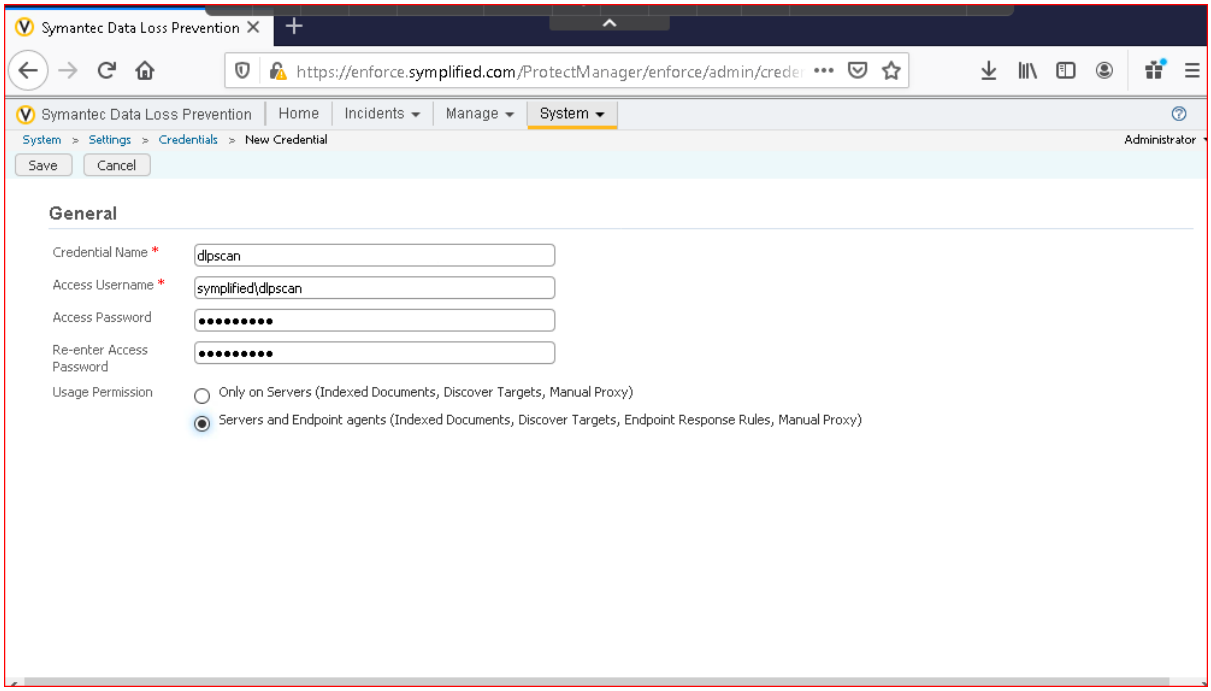
Results of the scan.

Exercise 2:

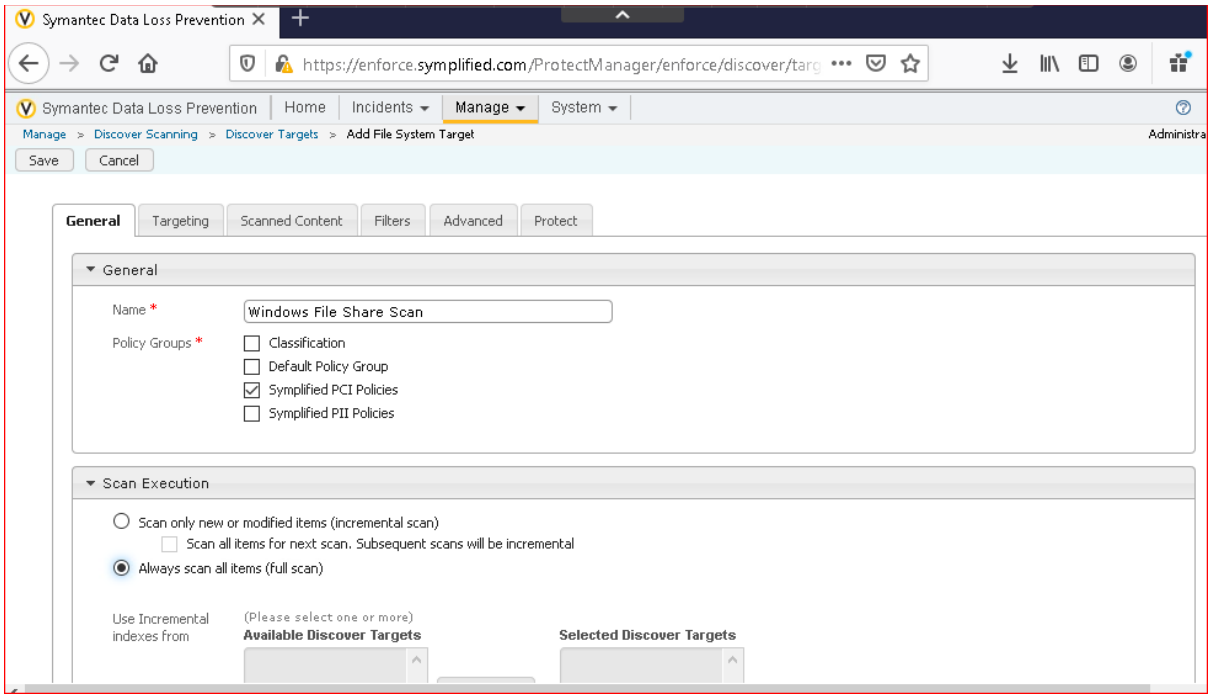
Scan a windows target

Whatever the data which is flowing through the network it should not be unencrypted and this scan analyses the data which is in the openshare.

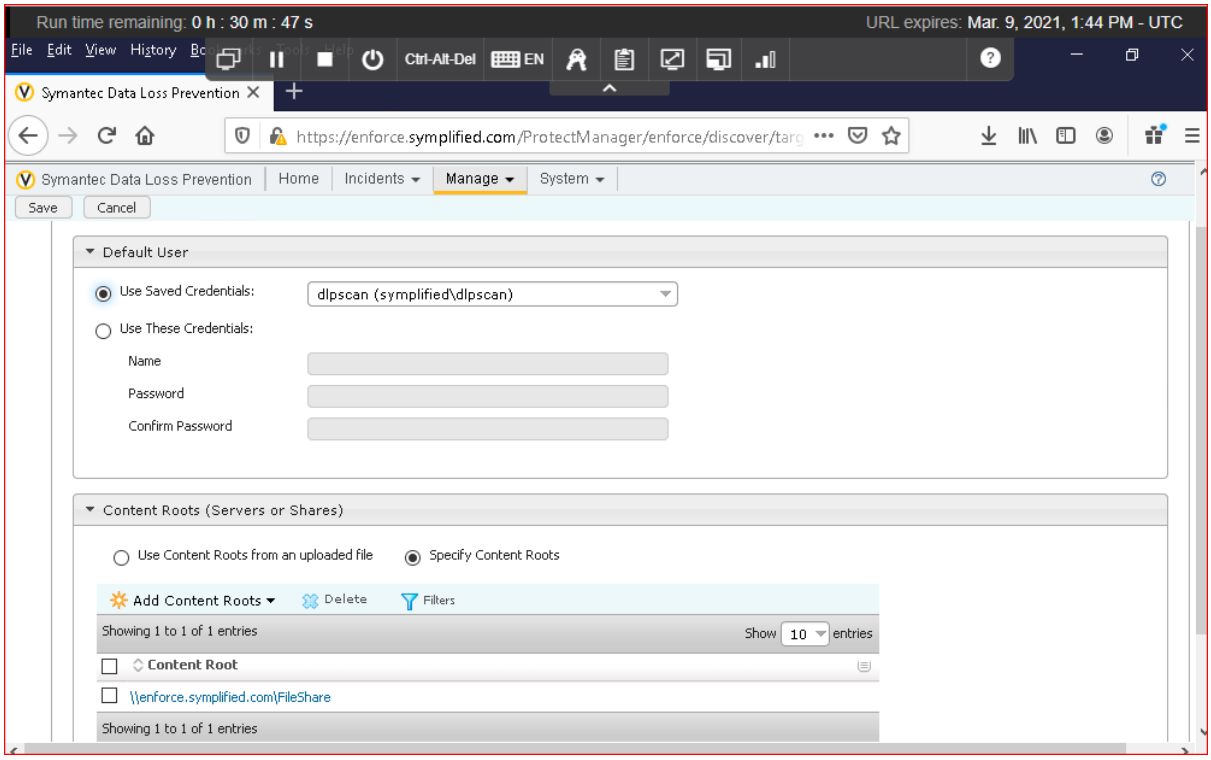
Vinay Kumar Reddy Donda dondavinayreddy@gmail.com



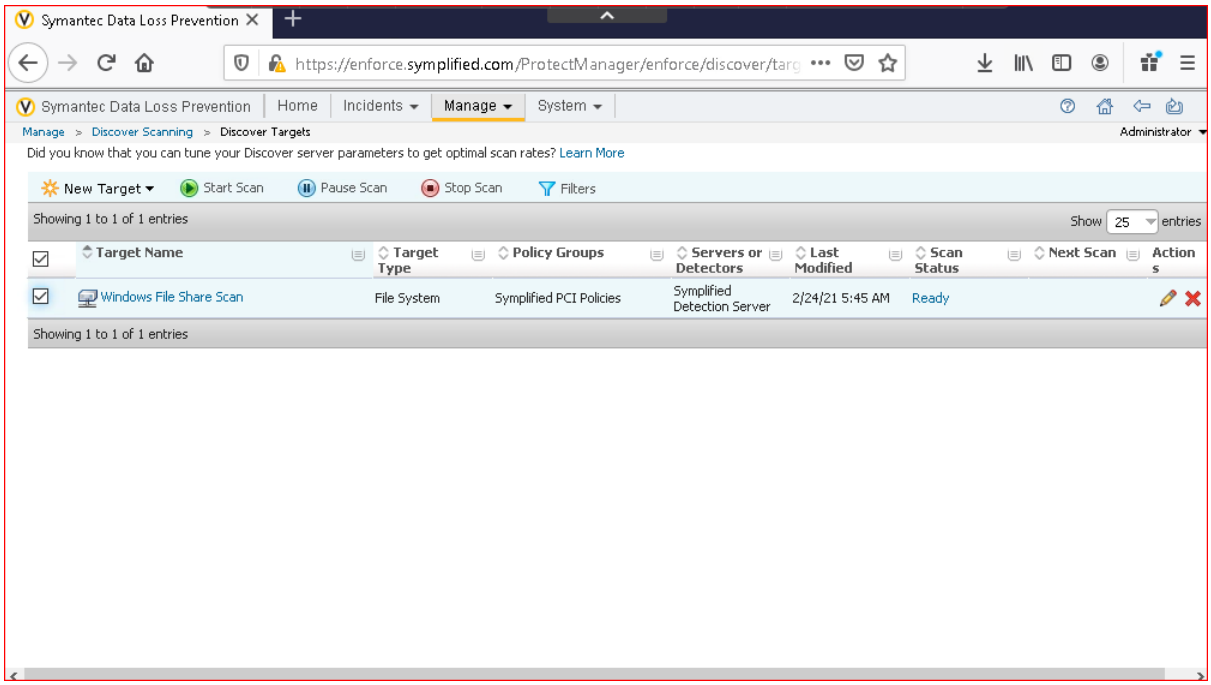
Adding credentials.



Adding details in the general tab.

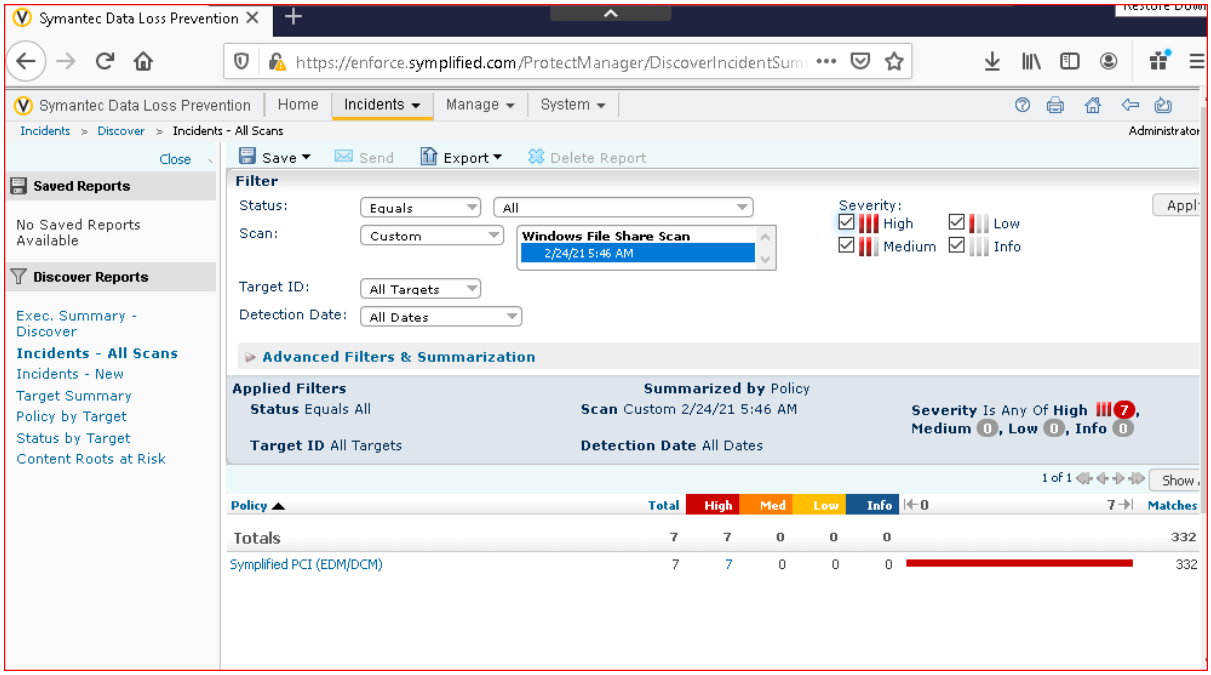


Adding the details in the scanned content tab.

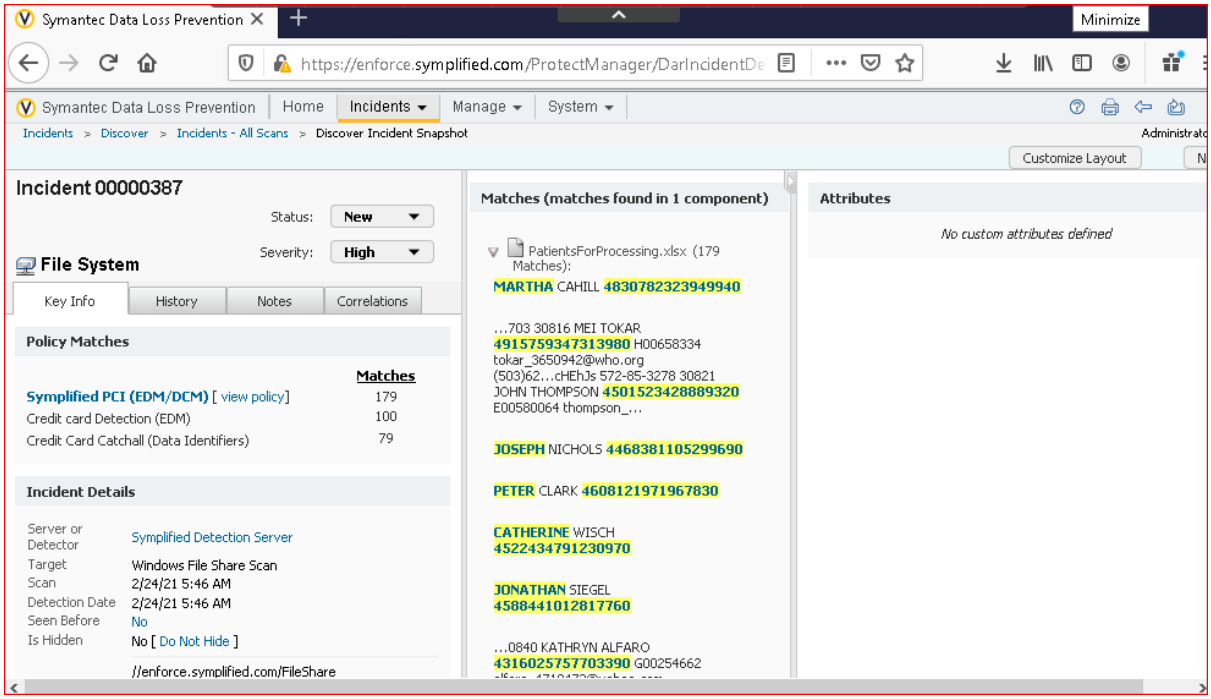


Added target and need to scan this.

Vinay Kumar Reddy Donda dondavinayreddy@gmail.com

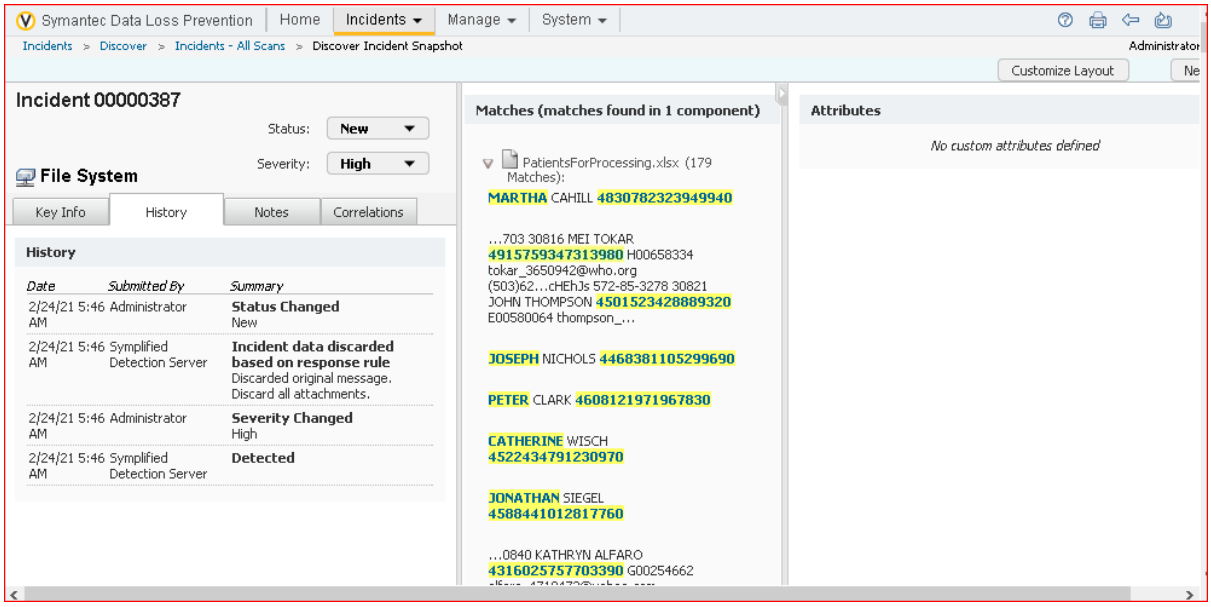


Result after the scan.



Incident page.

Vinay Kumar Reddy Donda dondavinayreddy@gmail.com



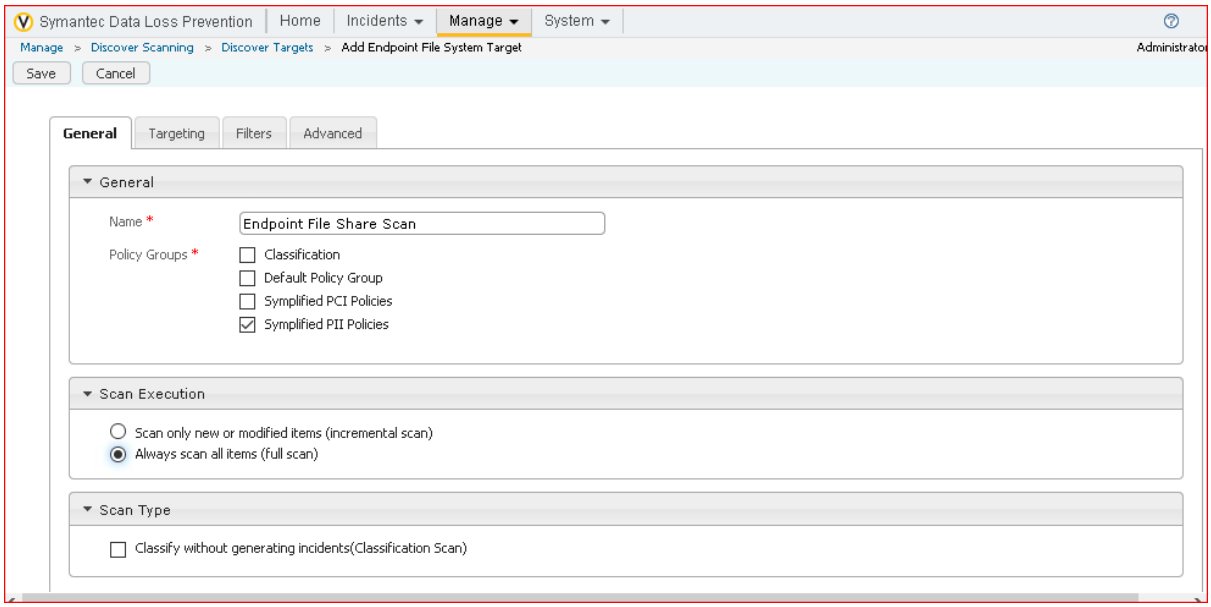
Seeing the history tab whether any actions taken on the incident.

Vinay Kumar Reddy Donda dondavinayreddy@gmail.com

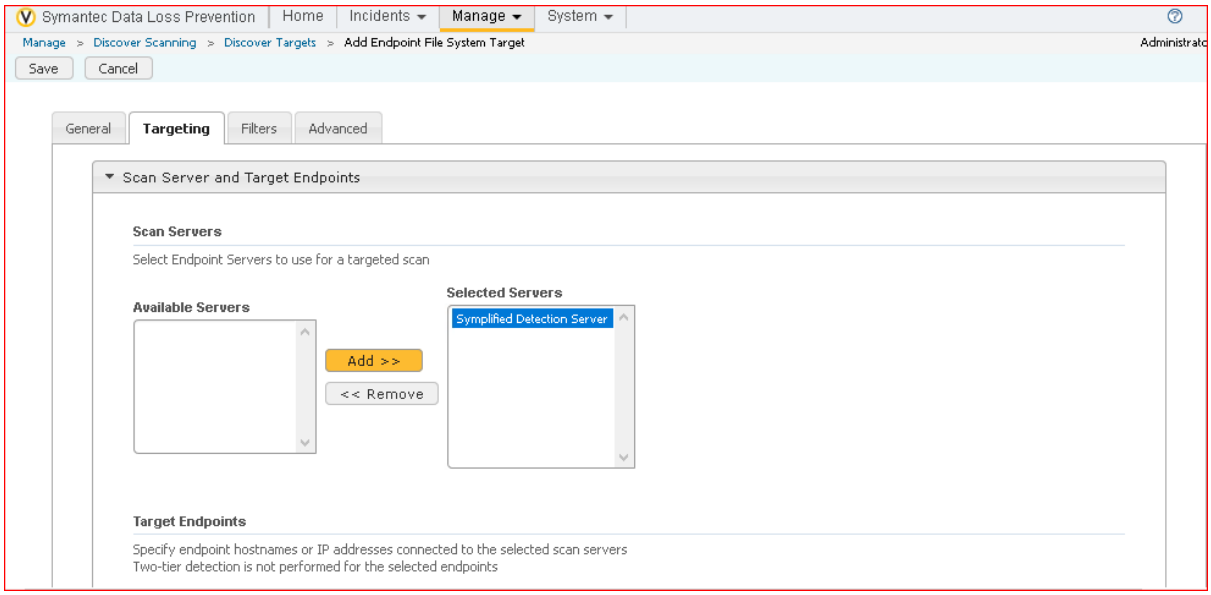
Exercise 3:

Scan endpoint computers for confidential data.

In a organization there will be many endpoints I mean there are many departments which uses the computer for their daily work for an IT guy it is difficult to manage all those so what we need to do is create and perform the DLP scan so that we can see the what confidential data is being stored in the respective endpoints.

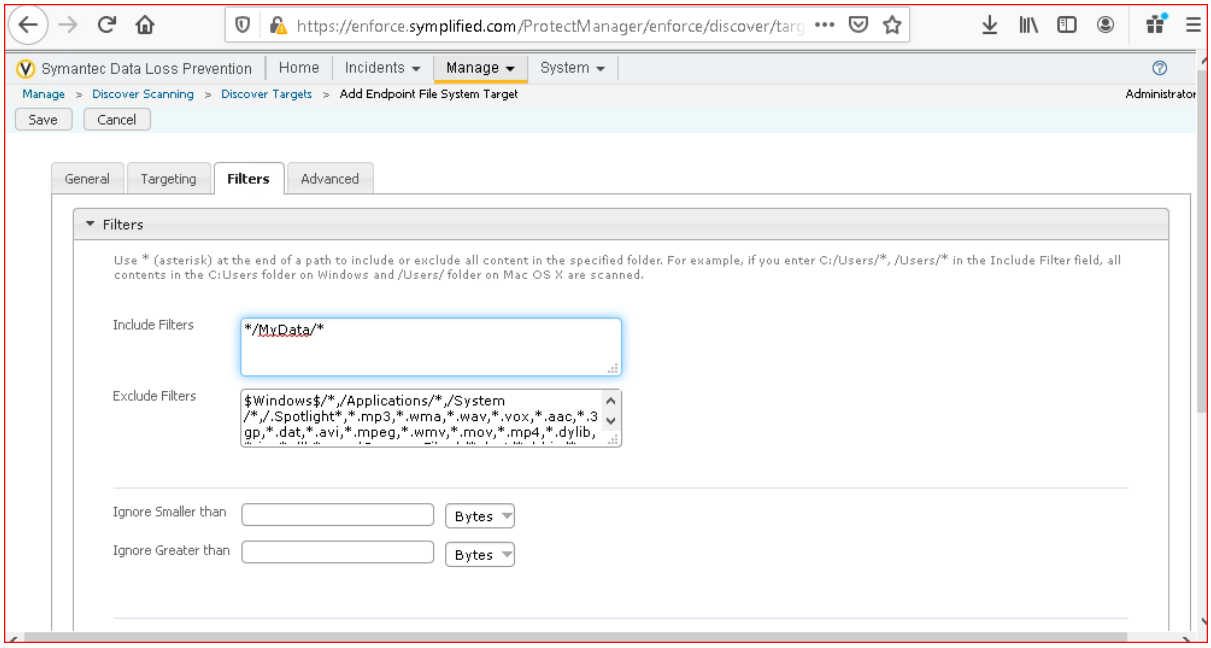


Setting rules in the general tab.

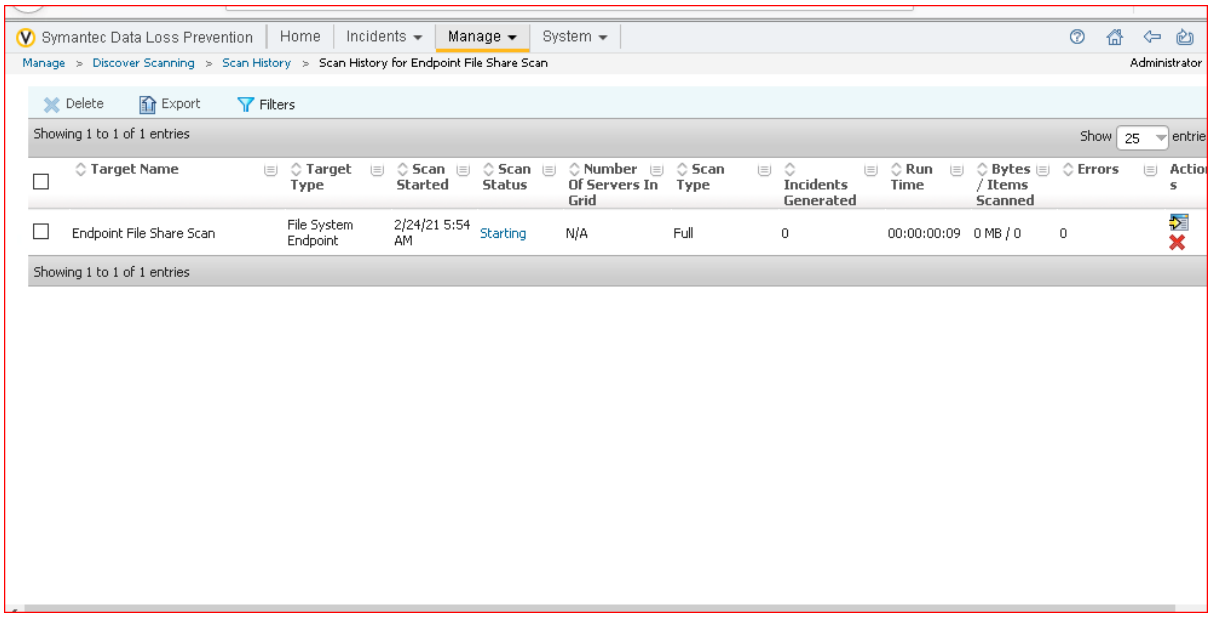


Setting rules in targeting tab

Vinay Kumar Reddy Donda dondavinayreddy@gmail.com



Setting rules in filters.



Scanning the Endpoint File share.

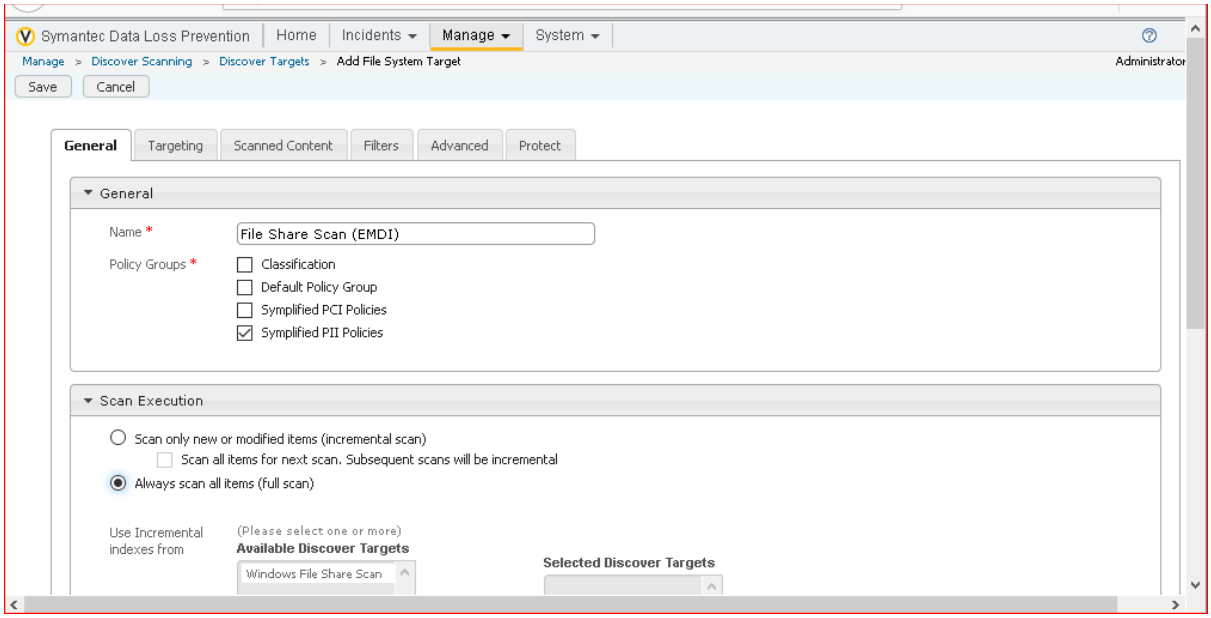
Exercise 4:

Scan server for confidential data using EMDI

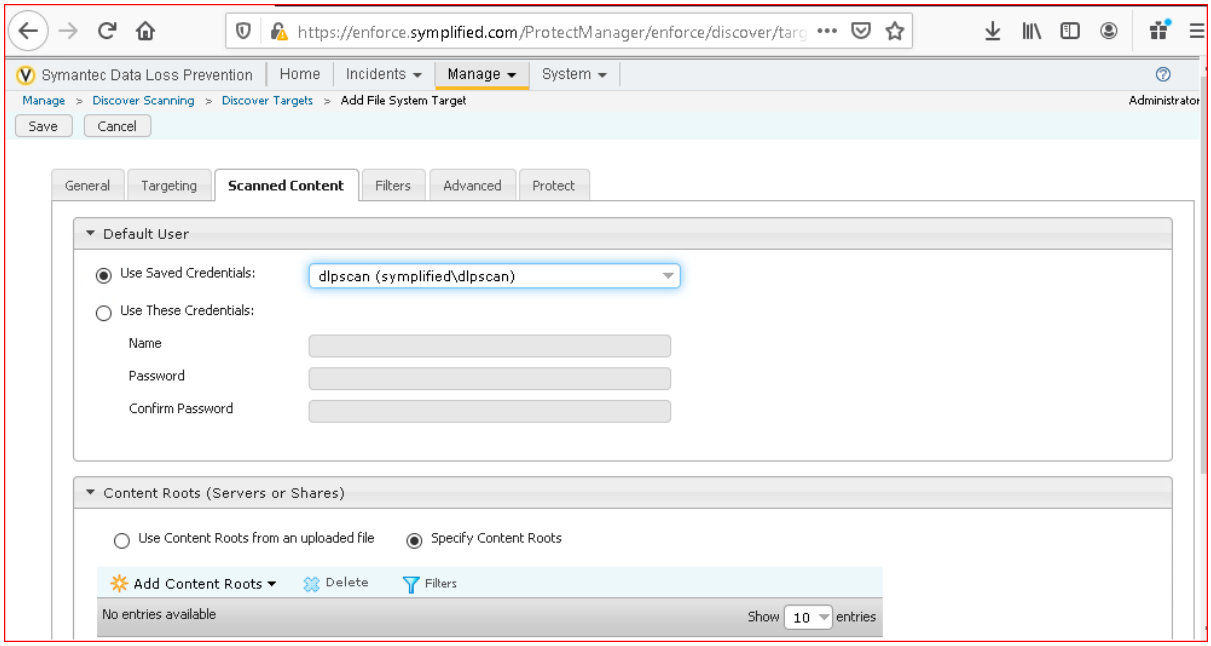
EMDI- Exact data matching.

This exercise is same as the exercise 3 of what we did the scan of the sensitive data but in this lab there is additional concept we are using and that is EMDI and purpose of this to uncut the un unimportant incidents when scanning the files on the endpoint computers.

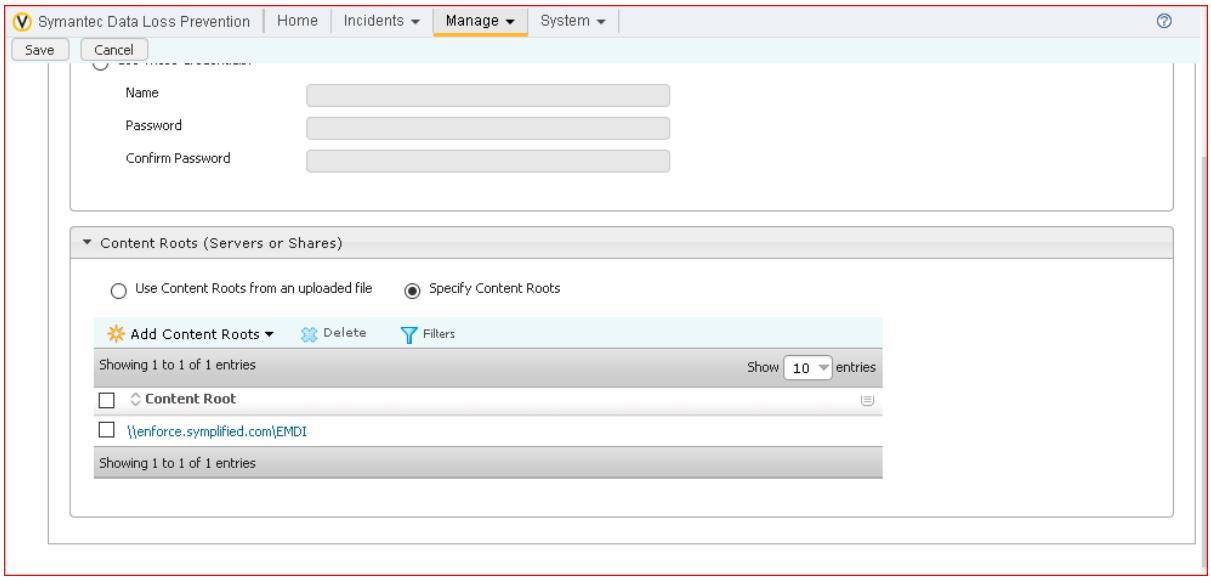
EMDI basically utilisies the data set which is there in the exercise 3 in order to validate the potential data breaches even before trigerring the incident.



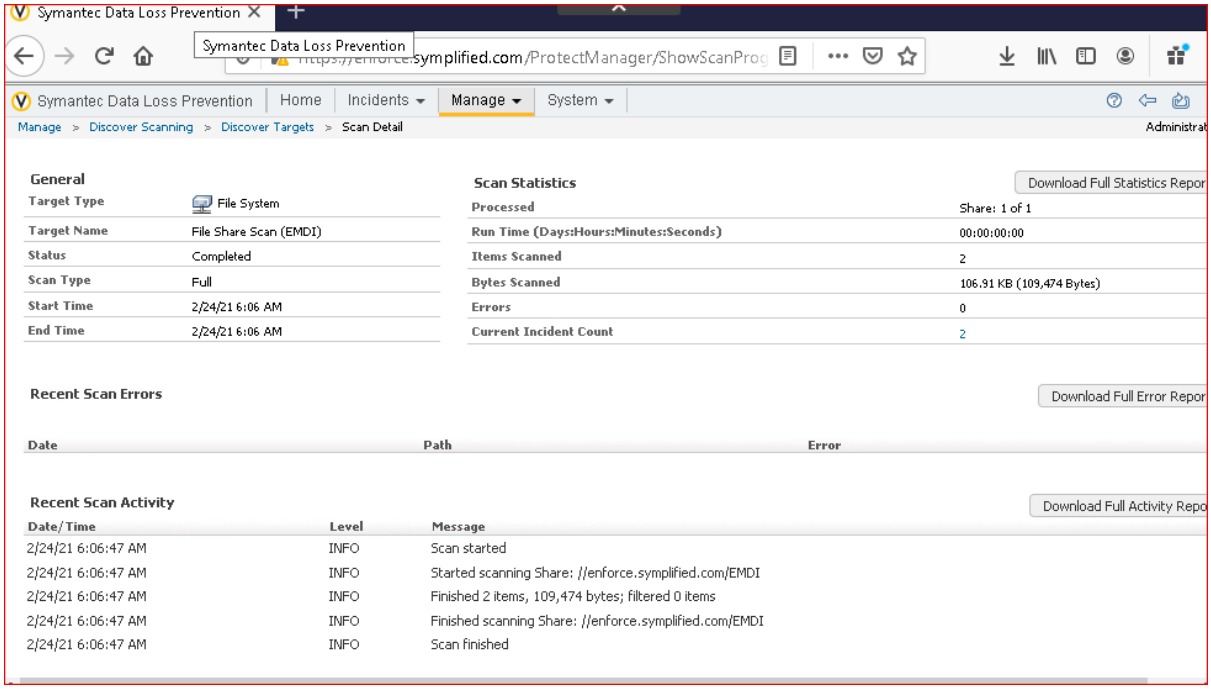
Adding the data in the general tab.



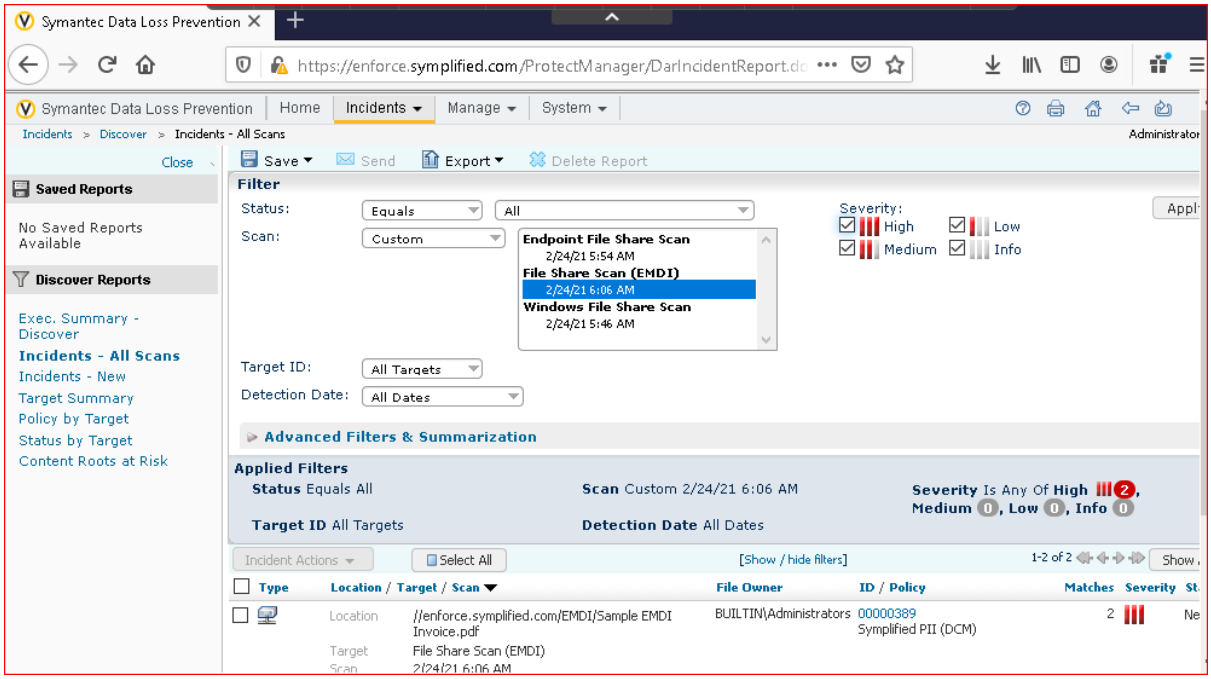
Adding data in the scanned content



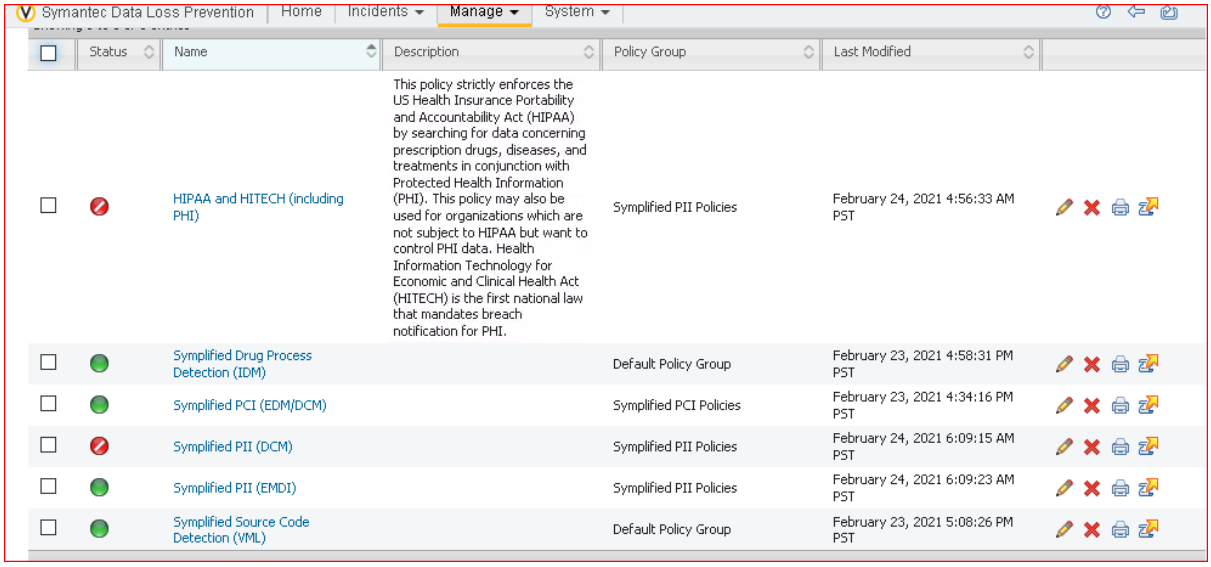
Adding the data in the scanned content.



Reviewing the scan statistics.

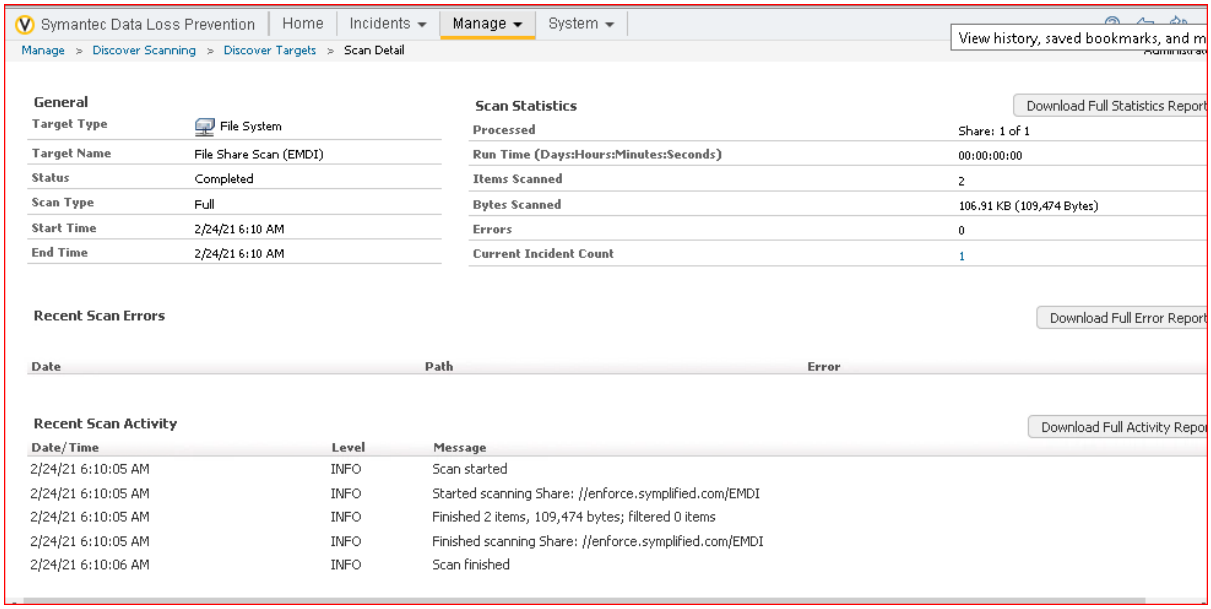


Here there are two incidents



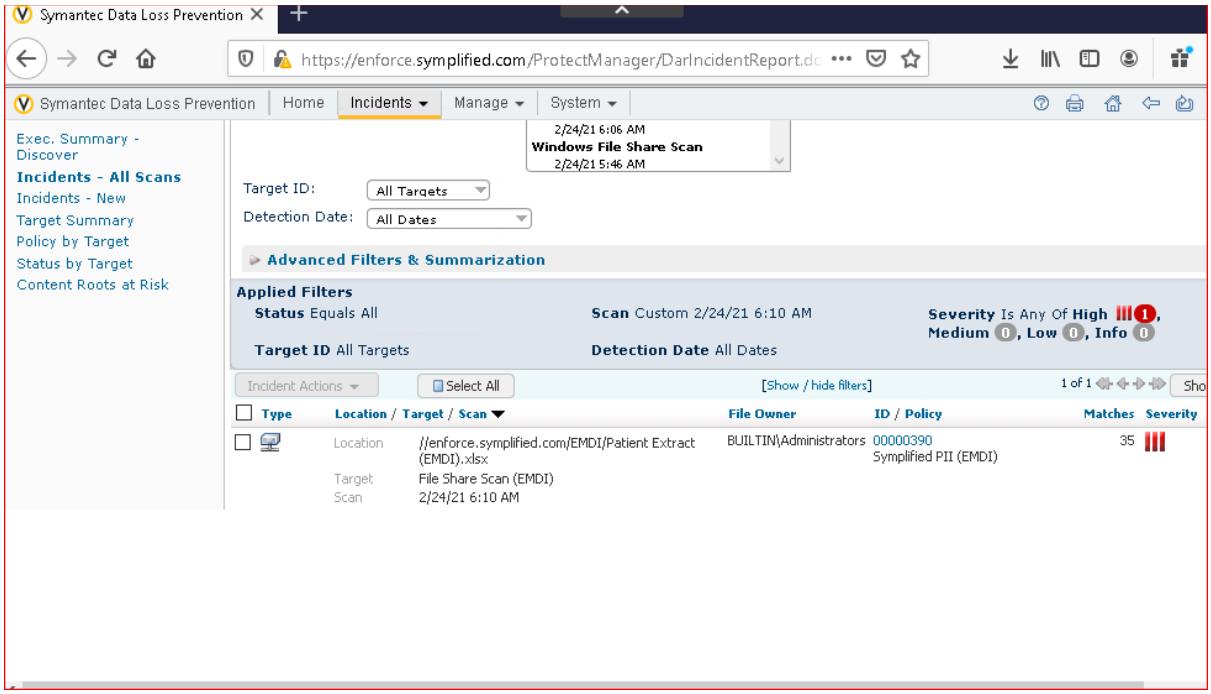
Activation and decativation is done.

Vinay Kumar Reddy Donda dondavinayreddy@gmail.com



Only one incident is discovered after activation and deactivation of rules

Symplied

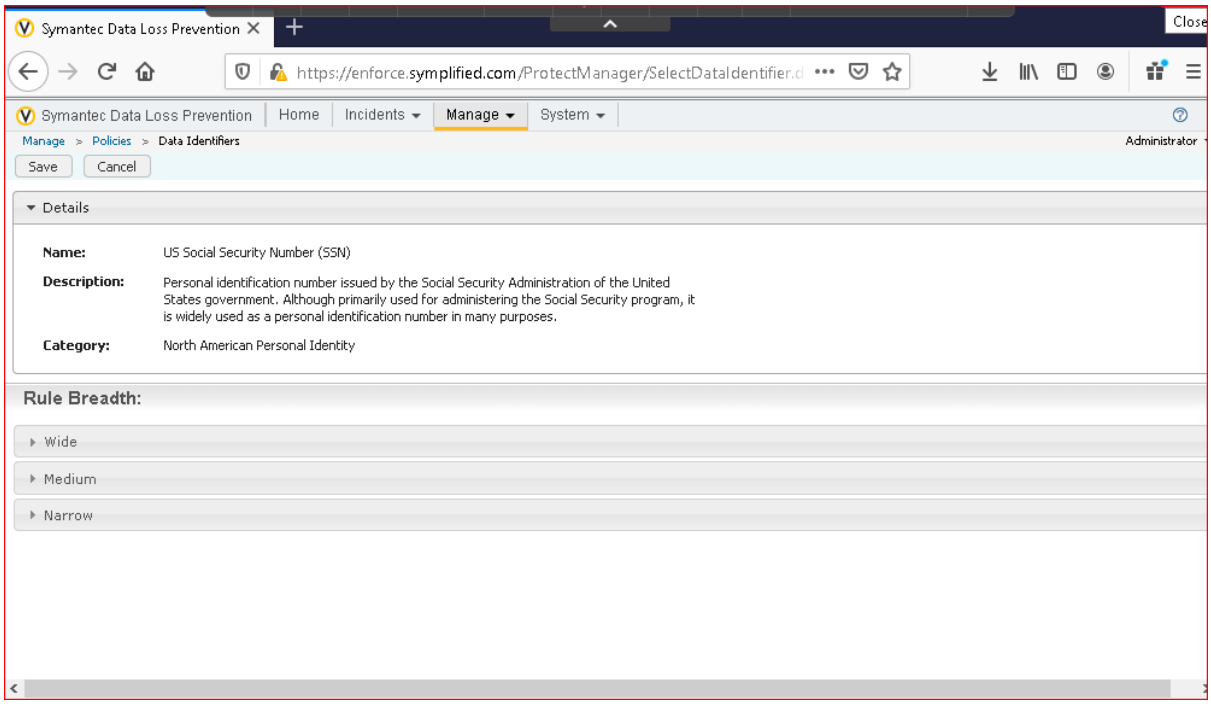


Displaying that one incident

Exercise 5:

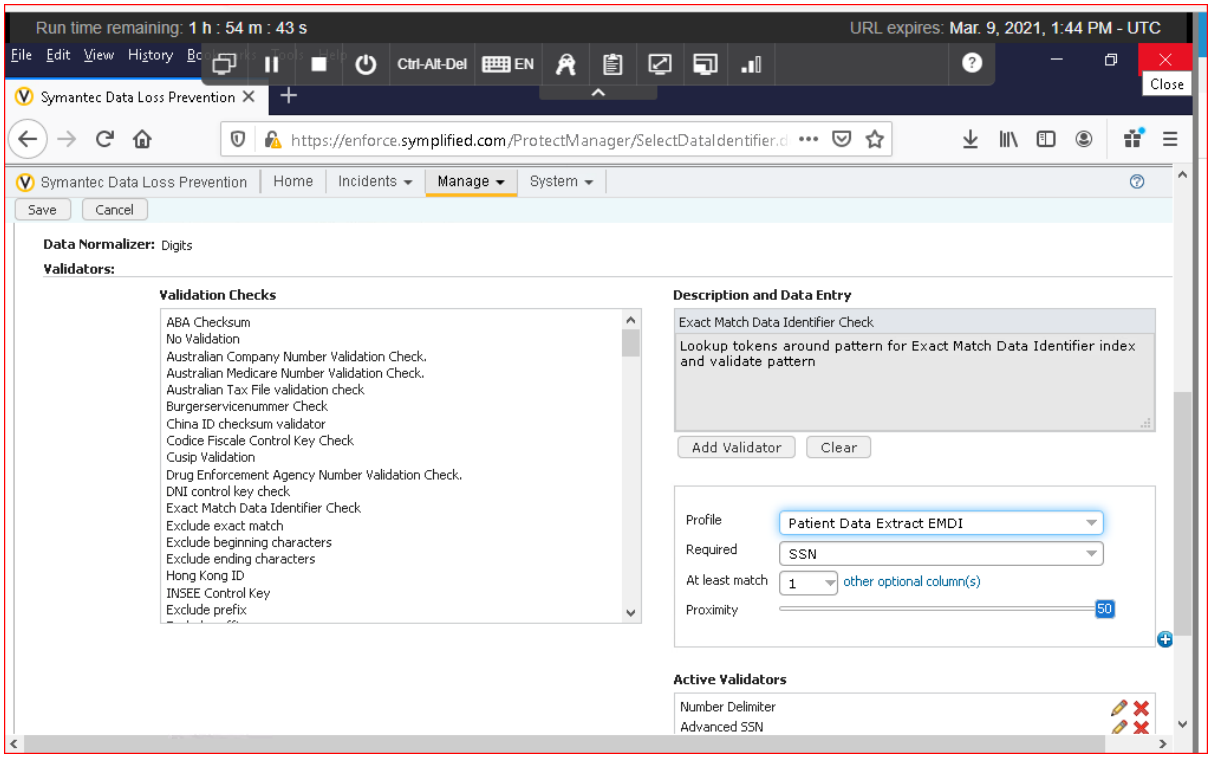
Configure a global policy for PII Compliance.

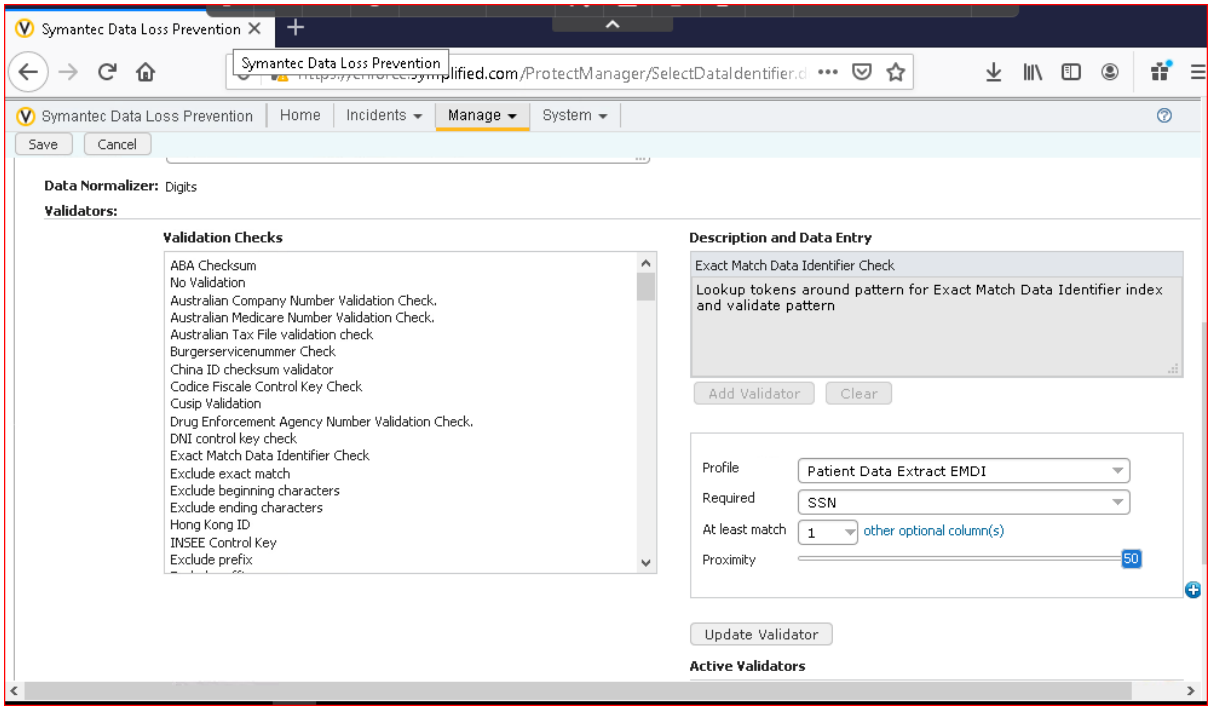
After using the Exact data match in the above exercise we understood how useful the Exact data match is. Since we add many policies in day – to- day life we use SSN numbers and EMDI would be very useful in additional validation check. Rather than adding this everytime I mean for each policy we need to create a global addition across the system so that a new policy can use the established data source.



US Social Security Number.

Vinay Kumar Reddy Donda dondavinayreddy@gmail.com





Section 3:

Understanding how confidential data is being used.

In this lab we use network prevent for email to monitor outgoing smtp messaged looking for important or confidential data that needs to be blocked or encrypted and we also monitor the user activity at the endpoints as well.

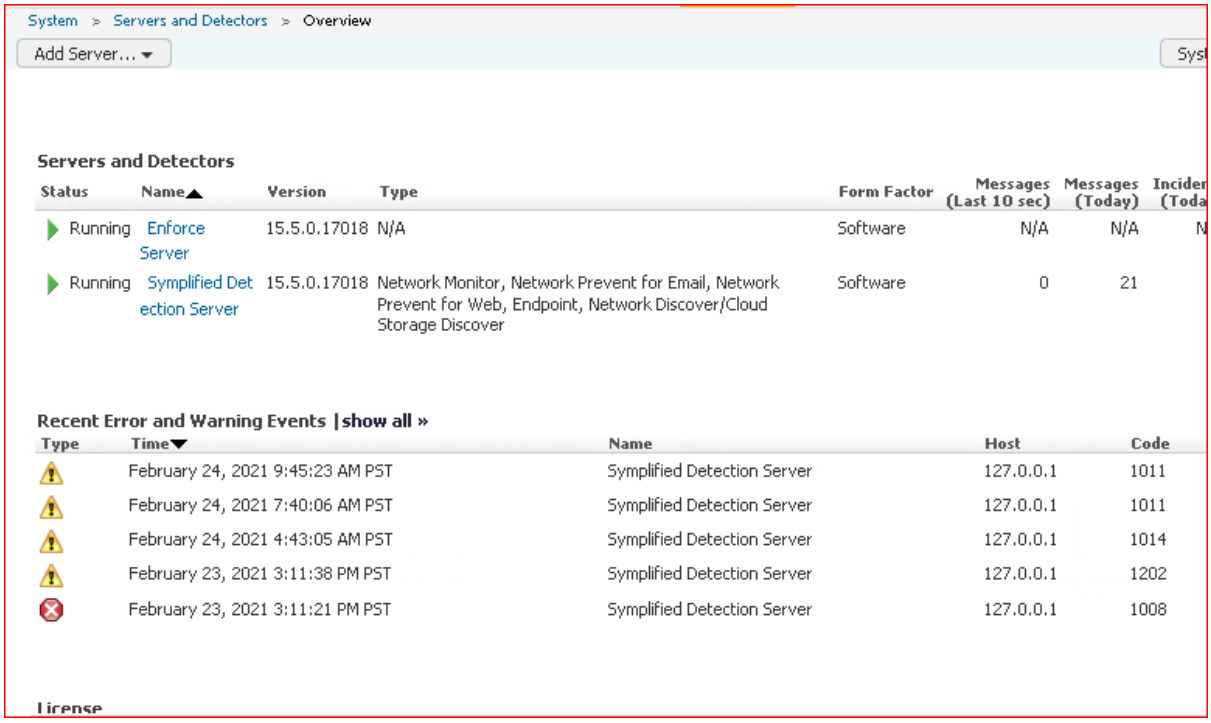
Exercise 1:

Configure Network prevent for email to monitor SMTP messages.s

The purpose of this lab is that no sensitive data should be leaked from the organization.

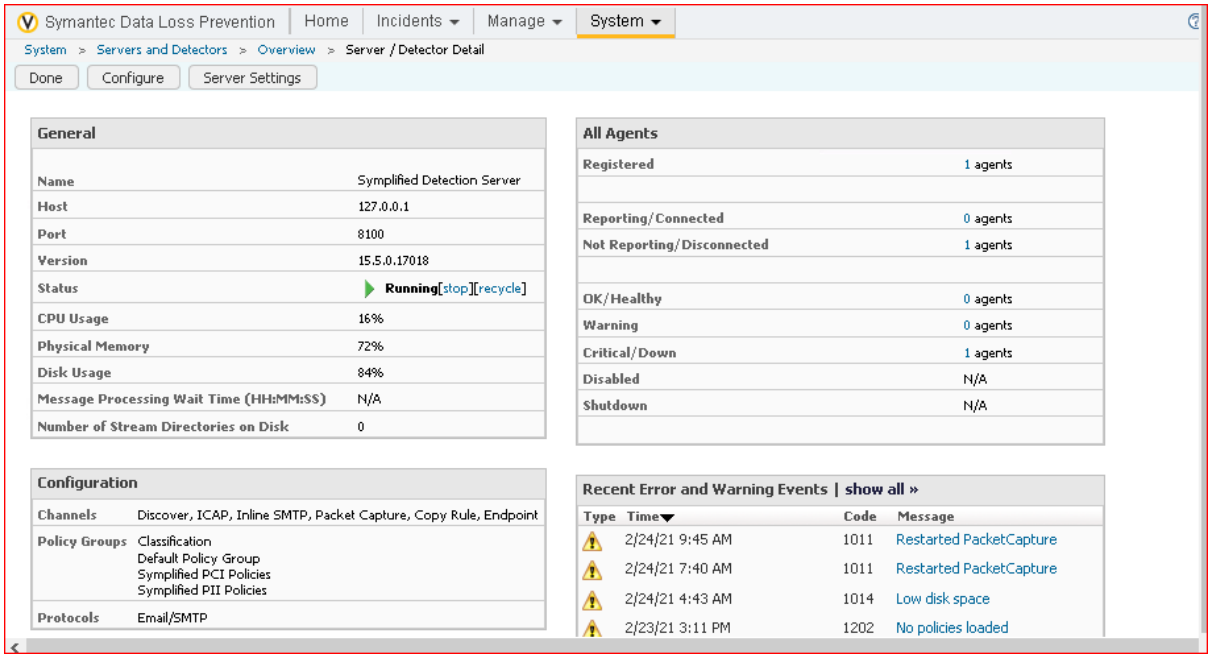
Any emails which contains the sensitive information leaving the organization unencrypted will be logged rather than blocked or rerouted.

It department will configure the DLP such that any emails containing the sensitive information should be re routed to the Symantec Encryption management server before sending to the recipient.

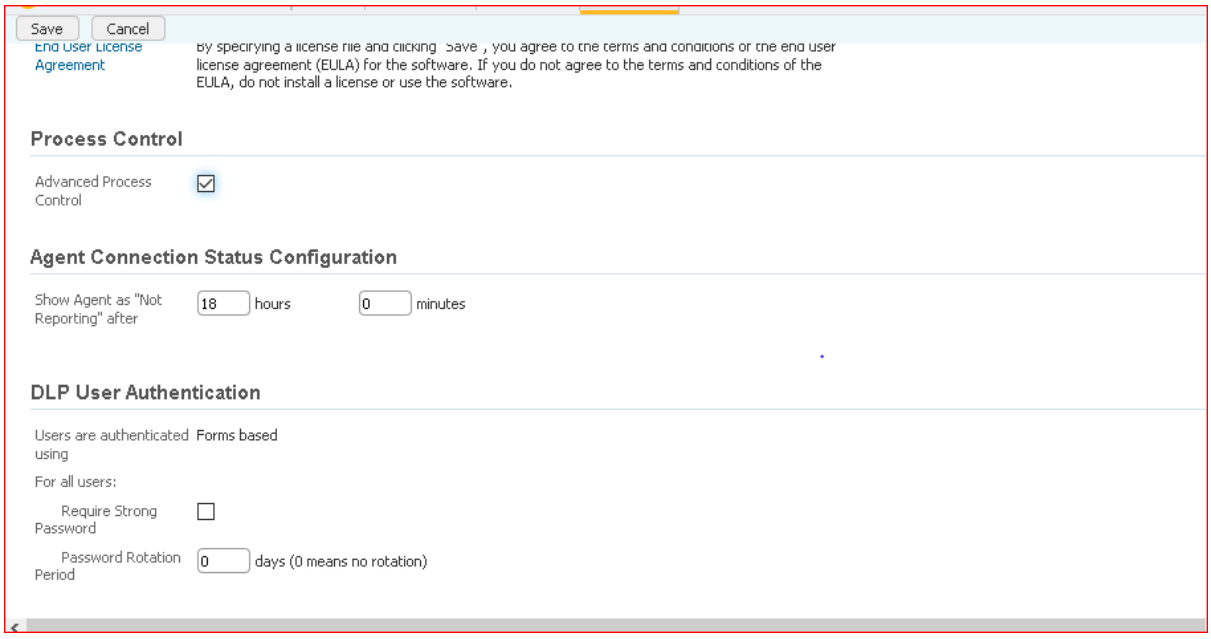


Now click on the simplified detection server

Vinay Kumar Reddy Donda dondavinayreddy@gmail.com

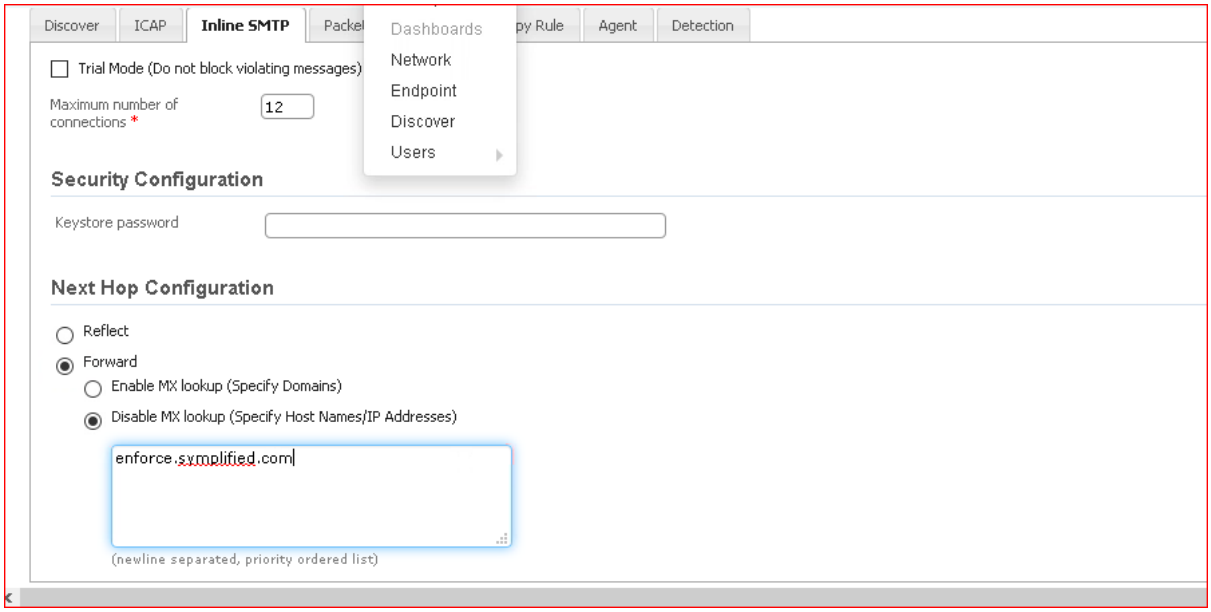


Simplified detection server details.

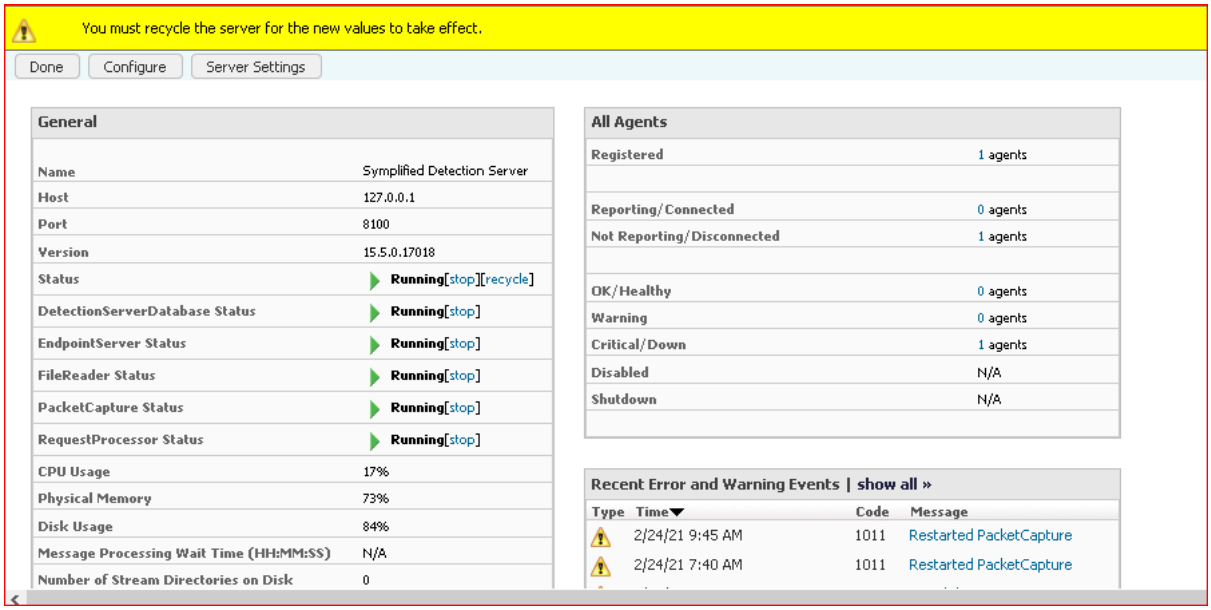


Selecting the advanced process control and click save

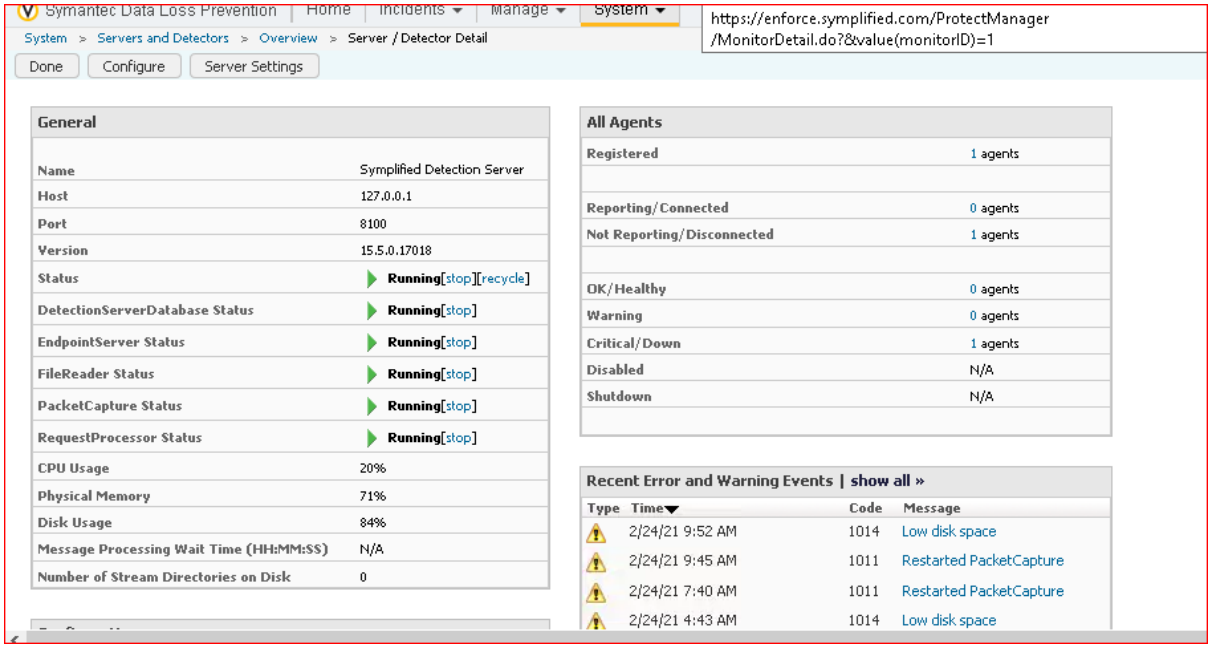
Vinay Kumar Reddy Donda dondavinayreddy@gmail.com



Rules in inline smtp



We need to recycle the server in order to apply the new rules.



After recycling all the status in general should be running and we can see that in above screenshot.

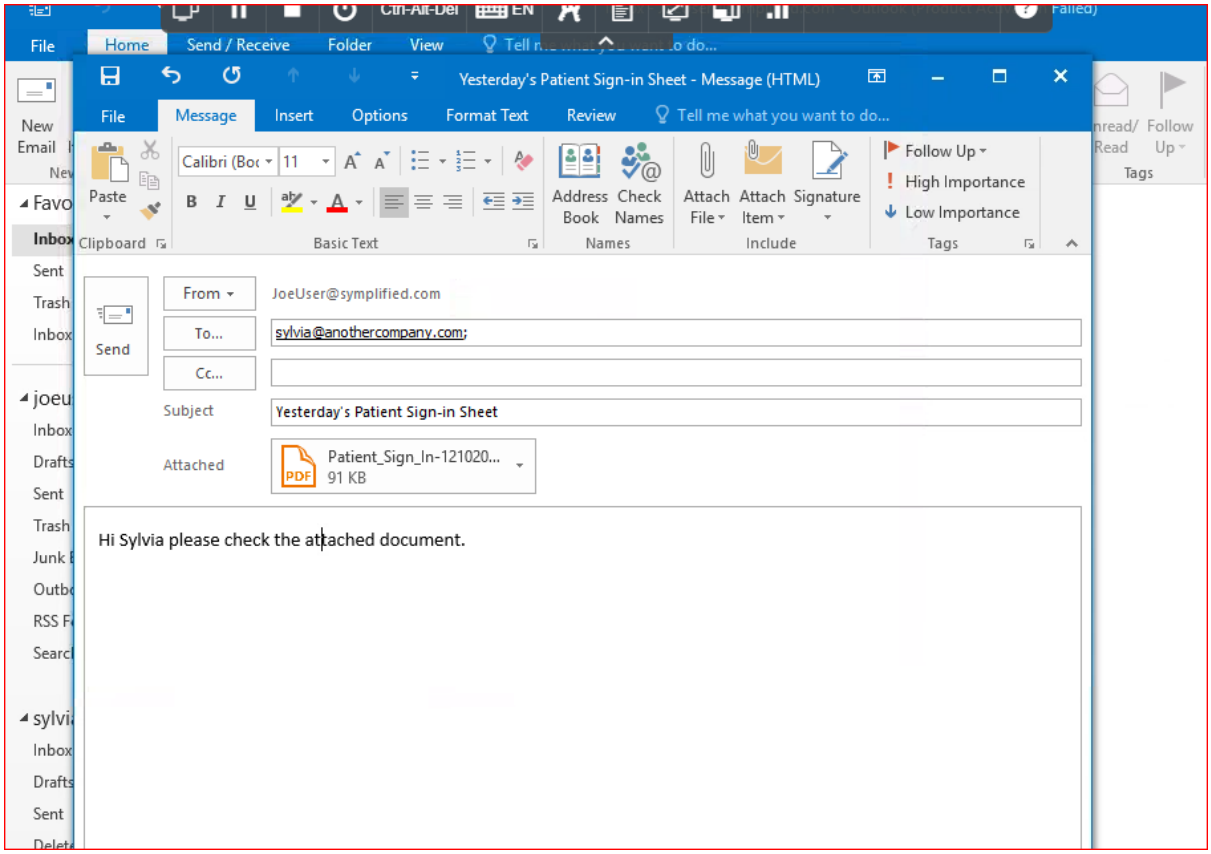
Vinay Kumar Reddy Donda dondavinayreddy@gmail.com

Exercise 2:

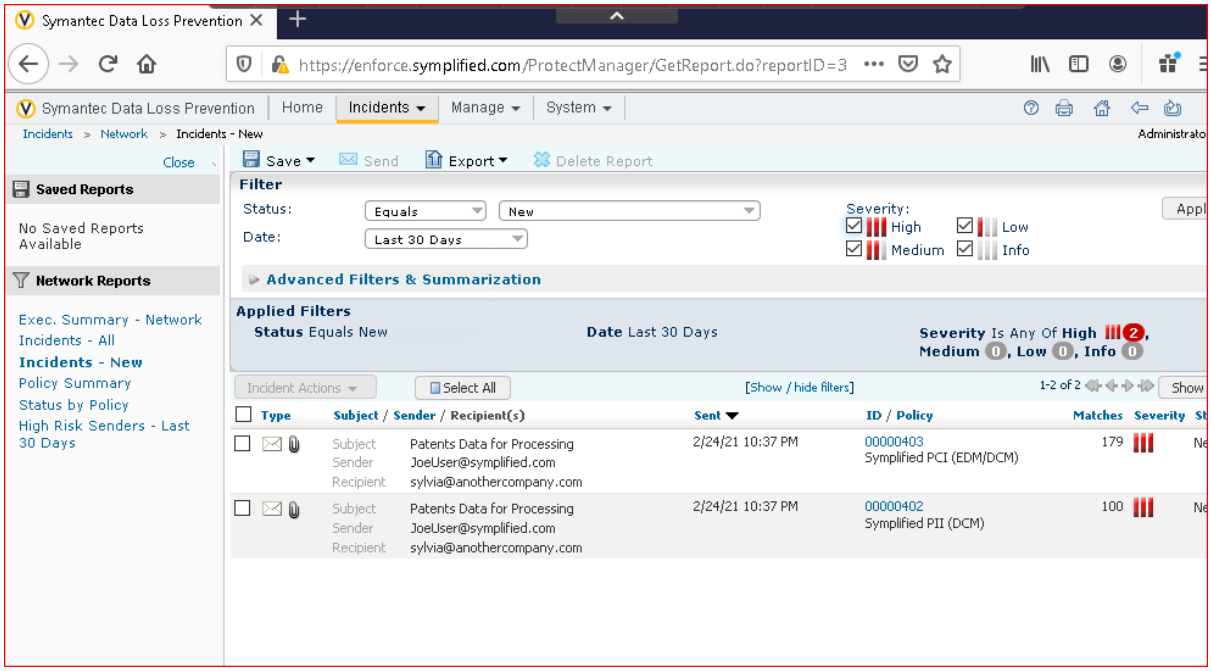
Use network prevent for email to monitor SMTP Messages.

In this lab user1 sends the email to the user2 first he sends the unsensitive data and next he sends the sensitive data so, in both the cases lets see for which incidents will be rised and how enforce server is gonna detect that.

This incident is raised when the sensitive data is transferring through the network.



Logged in as user joe and sending the mail to the syvlia which is not sensitive data.



While sending the insensitive data no incident is rised but while sending the sensitive data over the email incident is rising.

This incidents is raised in the networks not at the endpoint

Incidents at the network.

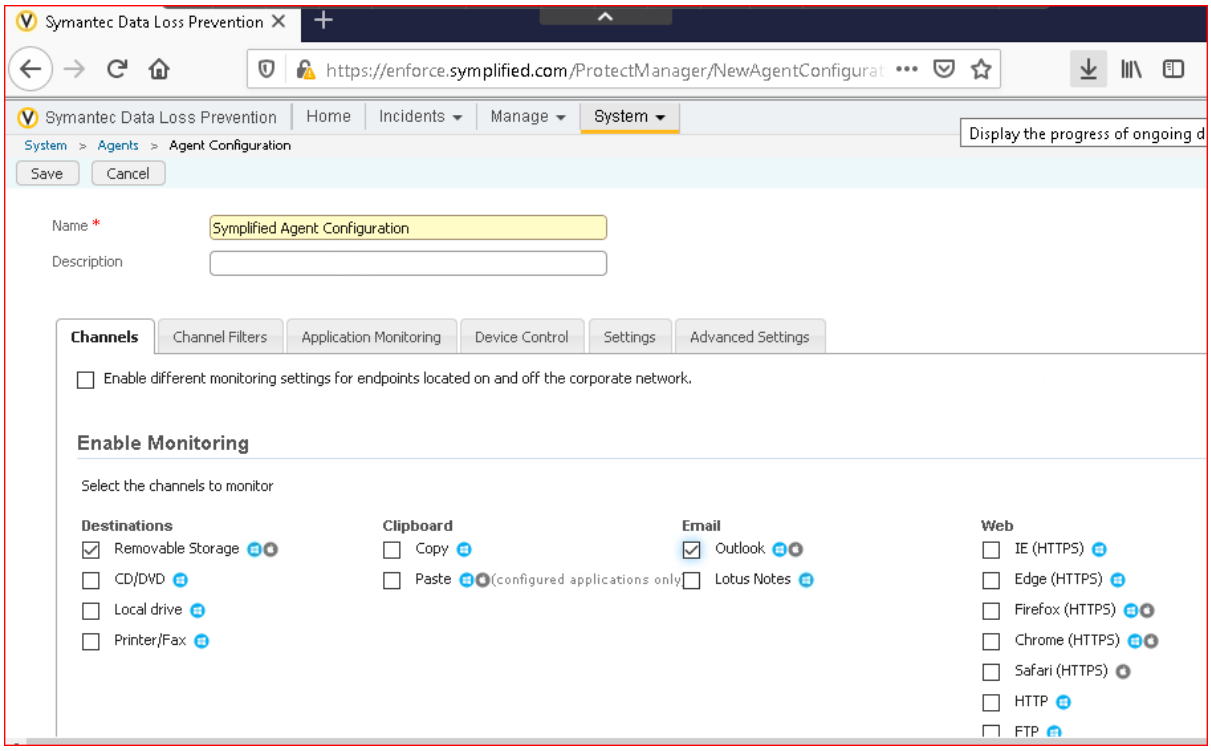
Exercise 3:

Monitor endpoint activity- Email

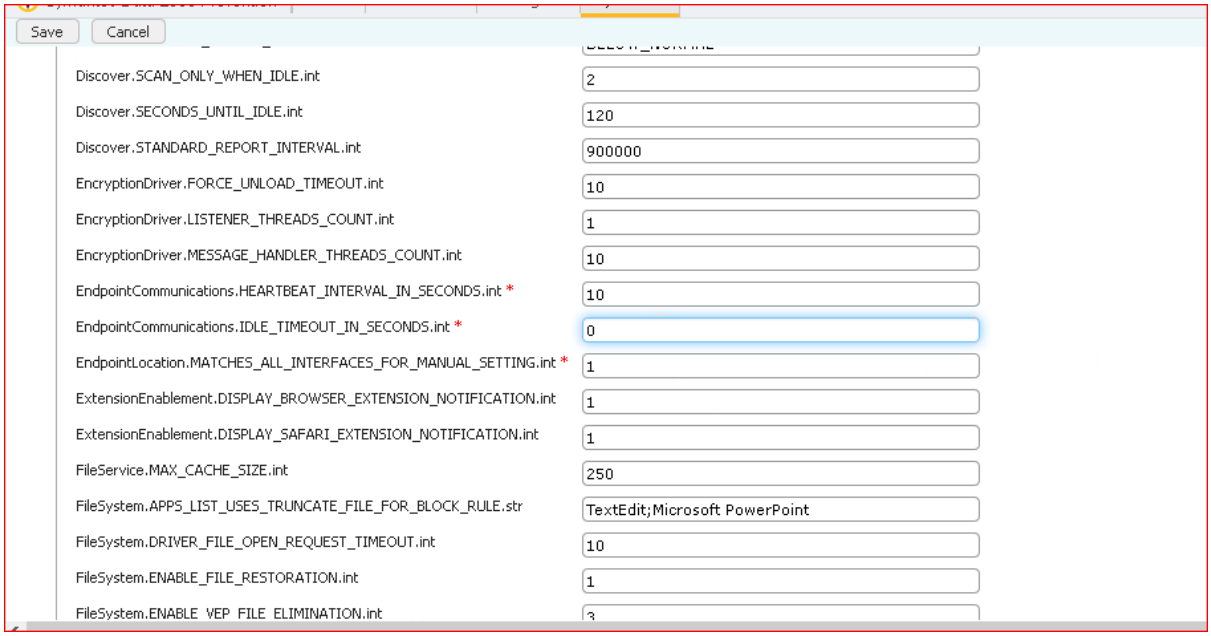
Network prevent for email has previously only used to monitor the emails at the networks but now monitoring at the end point is very much essential.

First point of security should be there at the endpoint and second point should be at the network. So always protect the data at the endpoints and next at the network.

In this exercise we use email monitoring to check email contents and attachements similarly how the network monitoring analyzed the email in the previous exercise.



Giving name and selecting outlook in channels tab

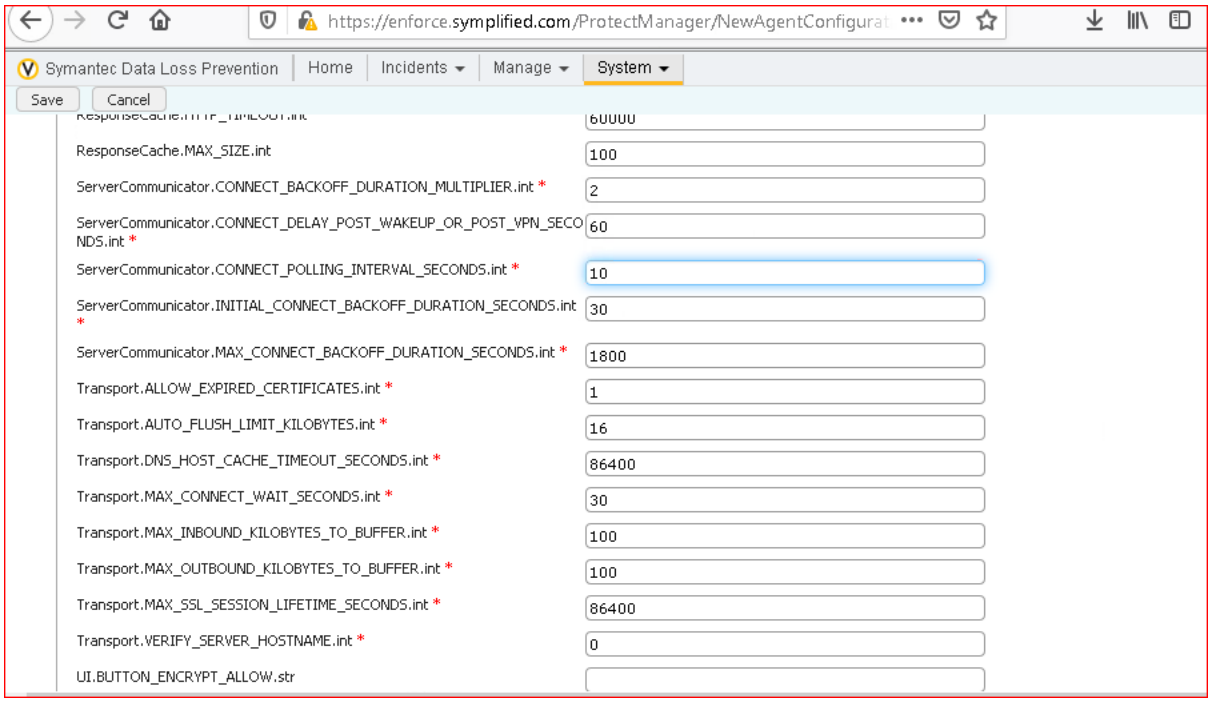


Changing the time in seconds for

EndppointCommunications.HEARTBEAT_INTERAVL_IN_SECONDS.int SECONDS TO 10

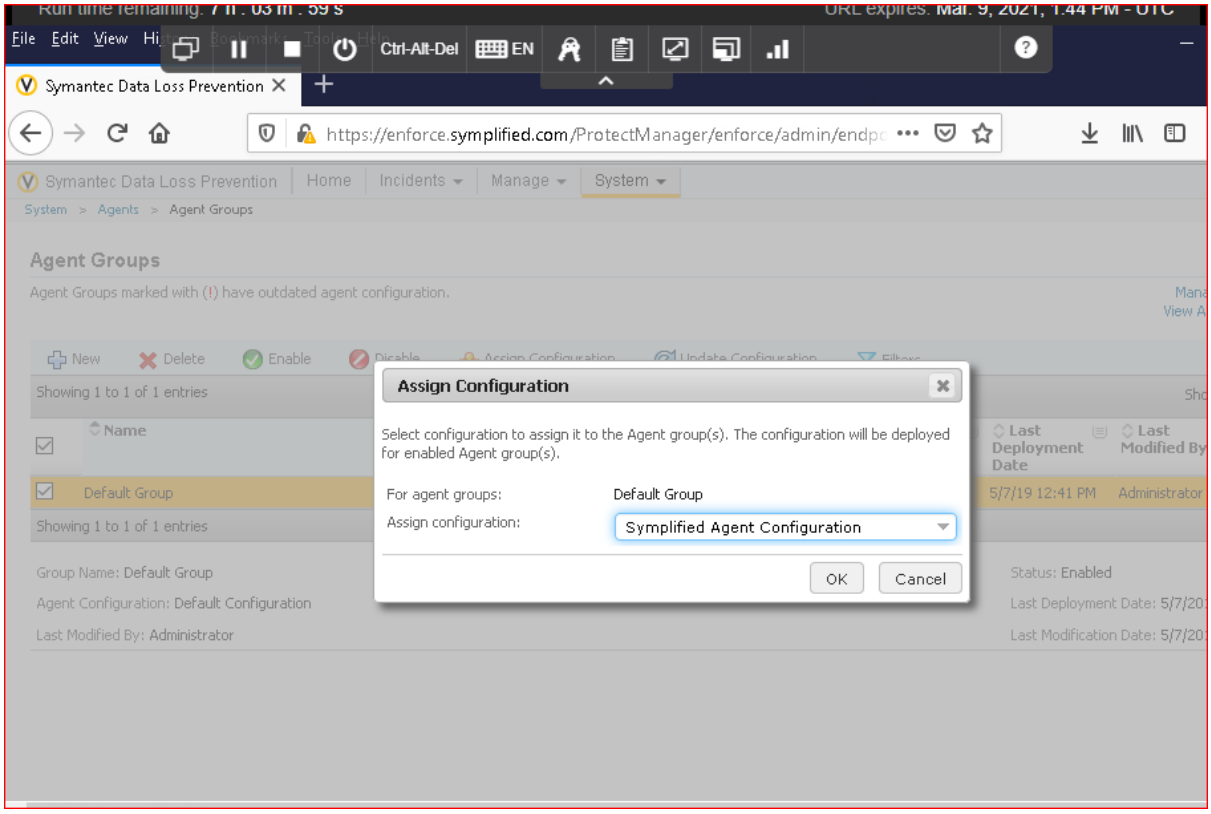
EndpointCommunications.IDLE_TIMEOUT_IN SECONDS TO 0

Endpoint

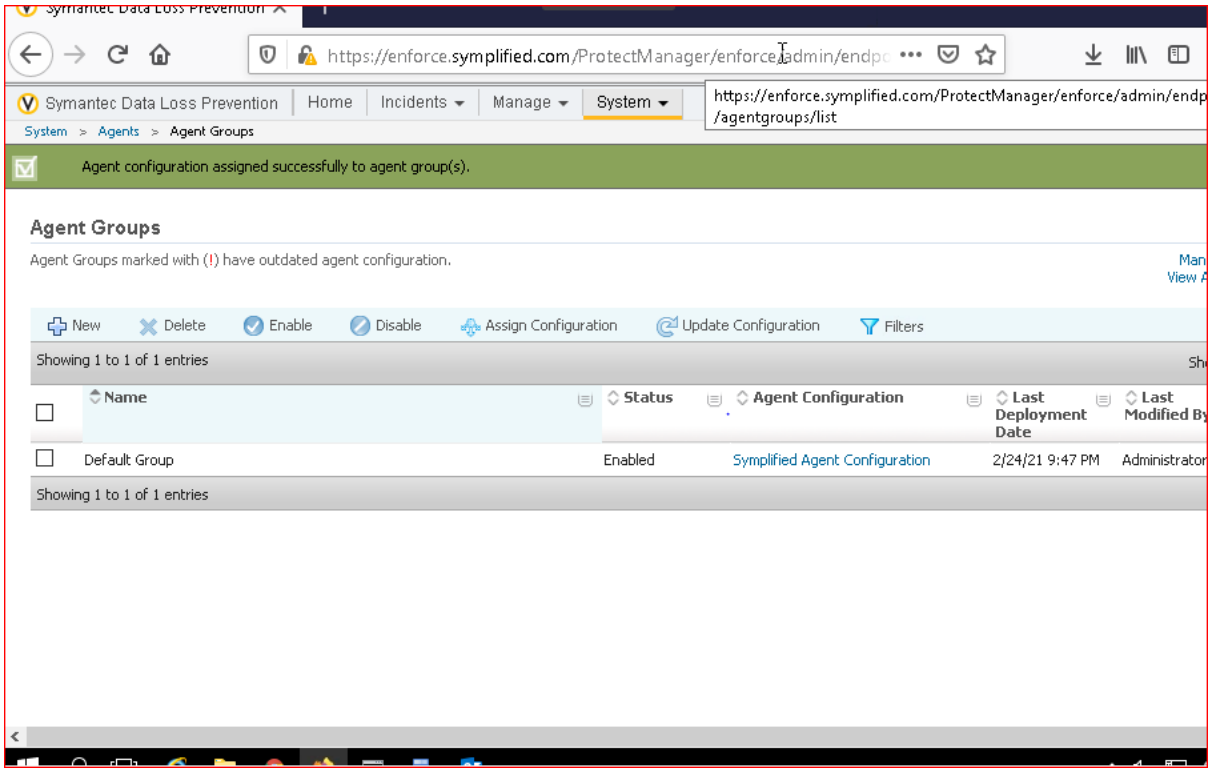


Configuring the setting

Setting server communicator.CONNECT_POLLING_INTERVAL_SECONDS.int to 10

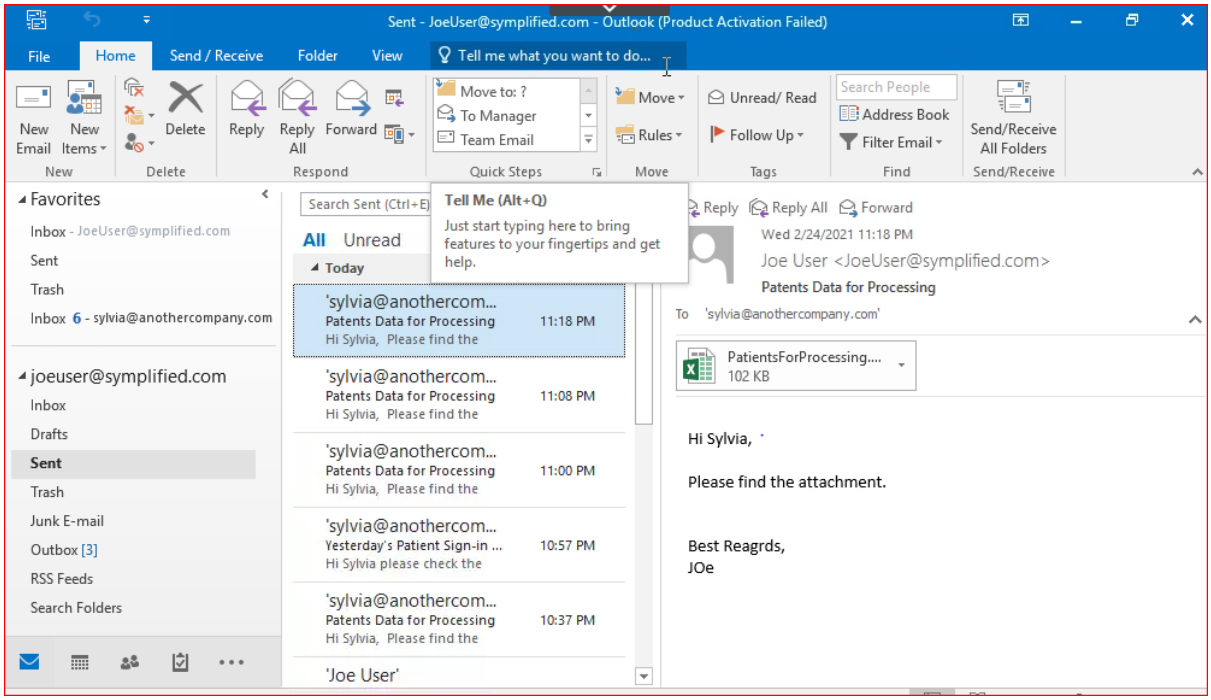


Updating the simplified agent configuration.

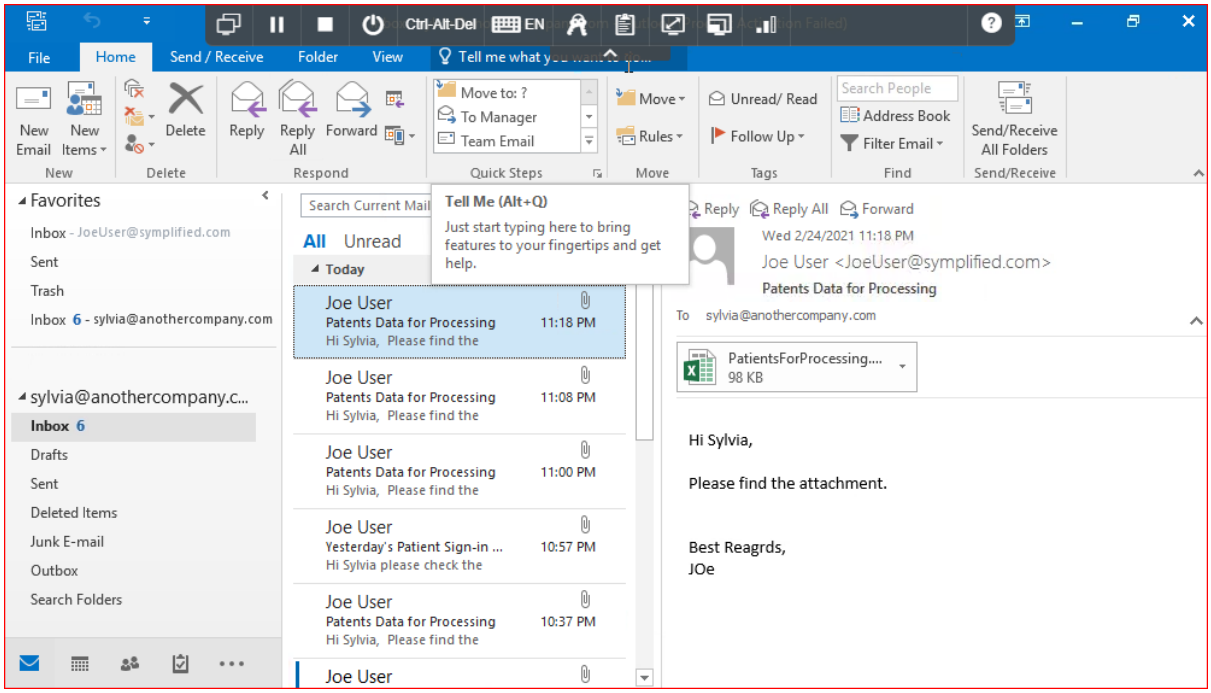


Since it is advanced setting we need to restart the device.

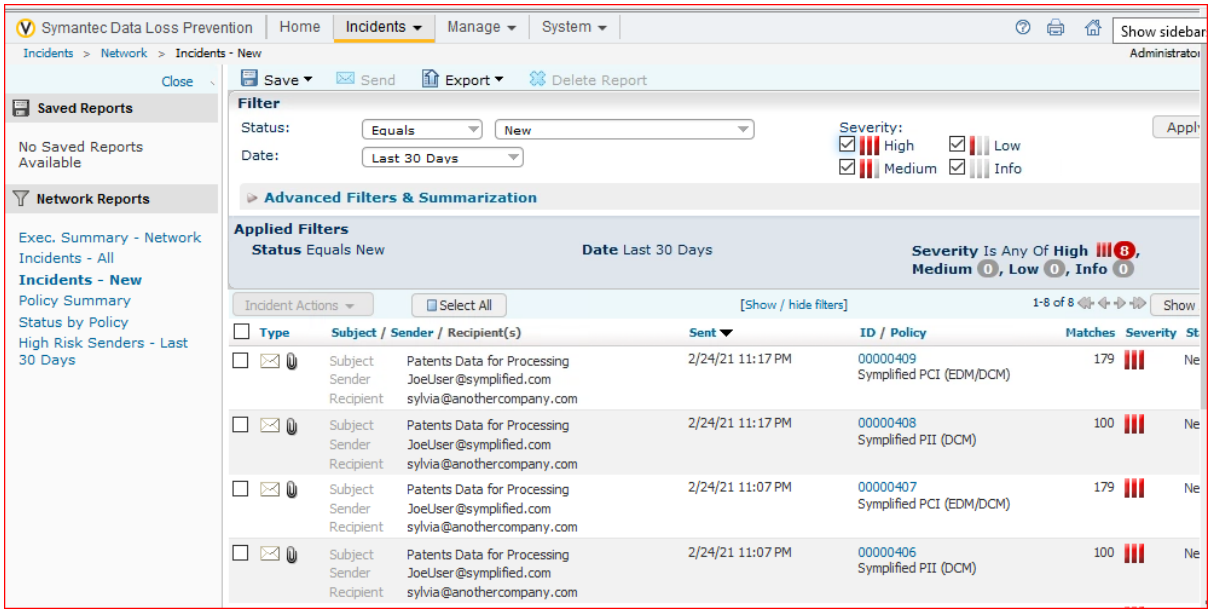
Vinay Kumar Reddy Donda dondavinayreddy@gmail.com



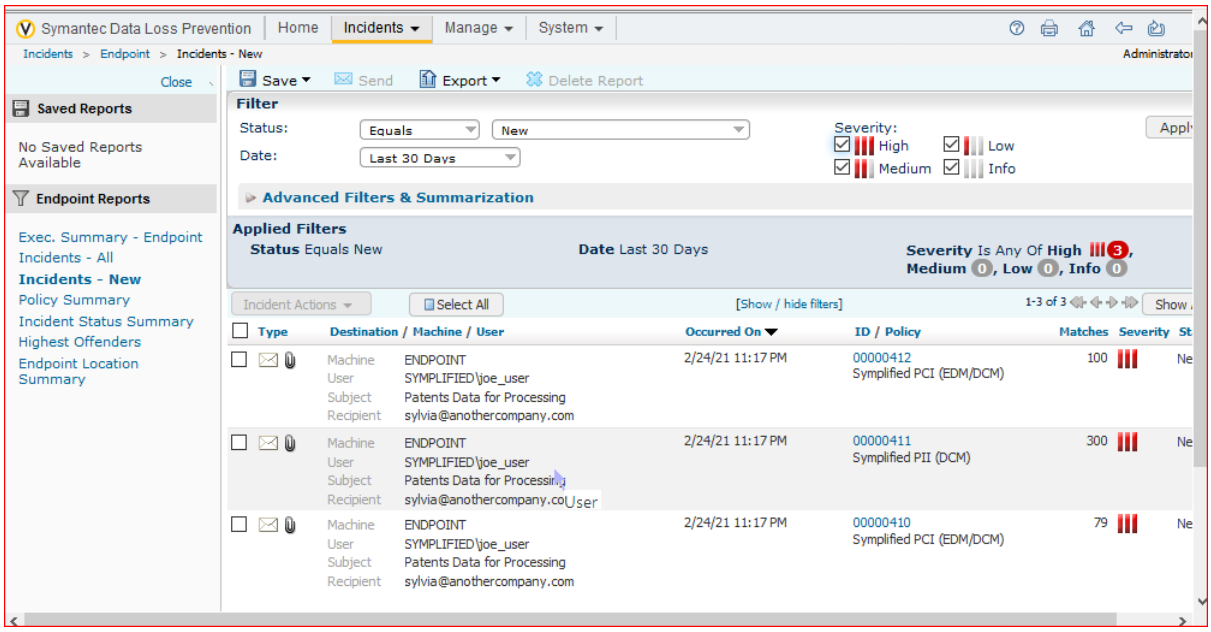
Sent message from joe to syvliva



inbox in sylvia



Incident is raised at the endpoint.



Incident is raised at the endpoint.

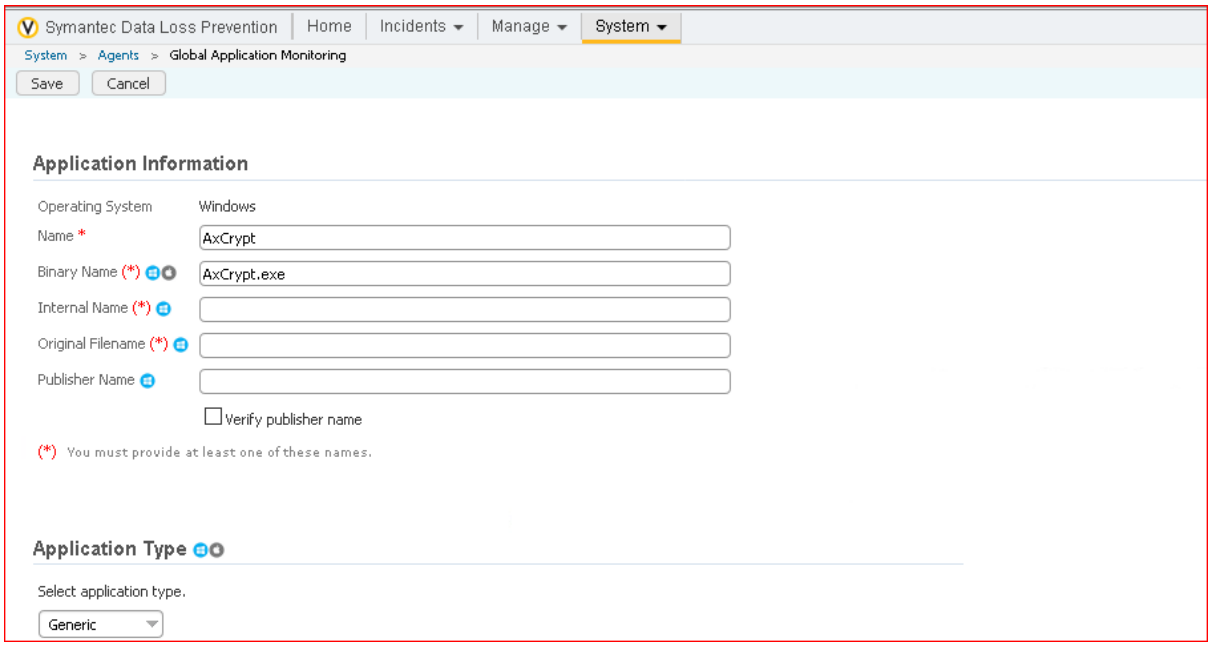
Vinay Kumar Reddy Donda dondavinayreddy@gmail.com

Exercise 4:

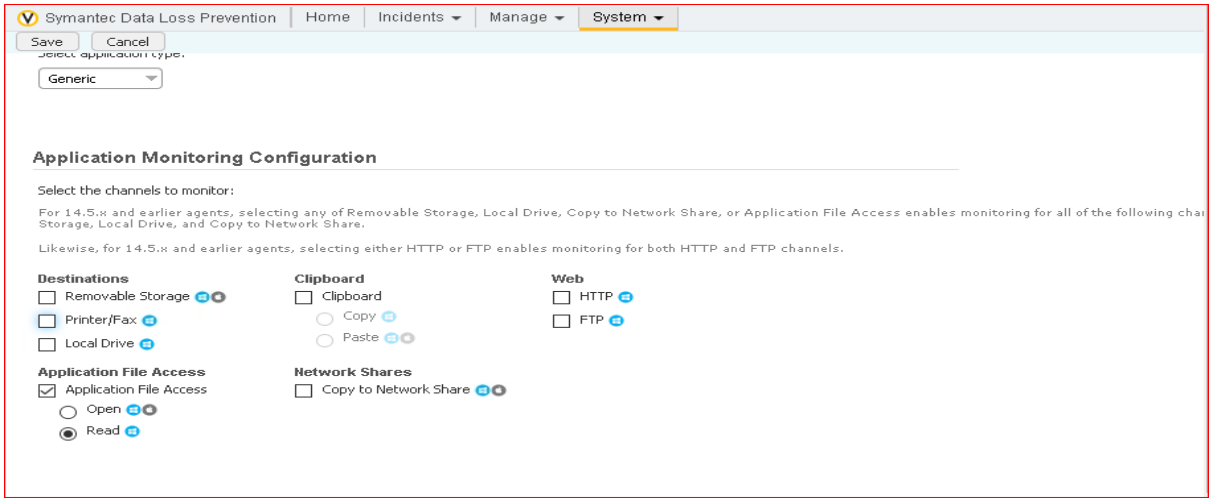
Monitor Endpoint activity – Third party apps

We know how important the sensitive data at the endpoints the best and easy solution is to use the Symantec DLP to monitor endpoints.

In this lab Application file Access control enables administrators to configure applications that are not pre-configured in Symantec dlp to be monitored the sensitive data usage. For suppose user joe want to encrypt the company's data with another application named AxCrypt but this application was not listed in Symantec DLP and its un authorized app which can steal the company's sensitive data. So company observed this thing and used the Symantec DLP such that no data is encrypted is using the other applications apart from which is listed in the Symantec DLP.

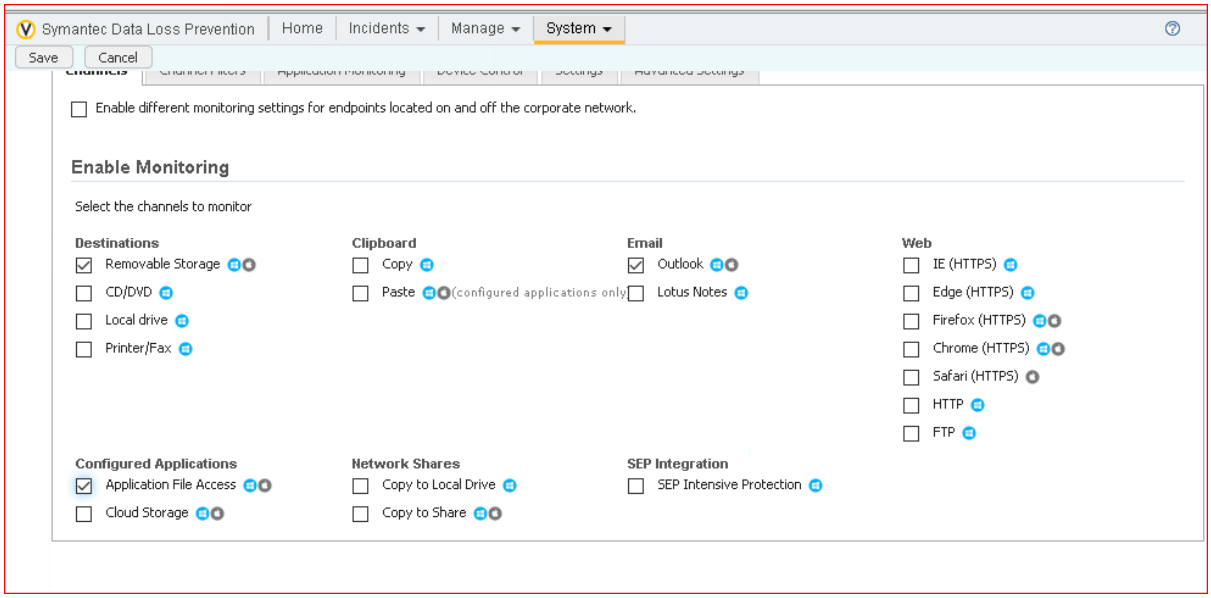


Adding the application in order to block that.

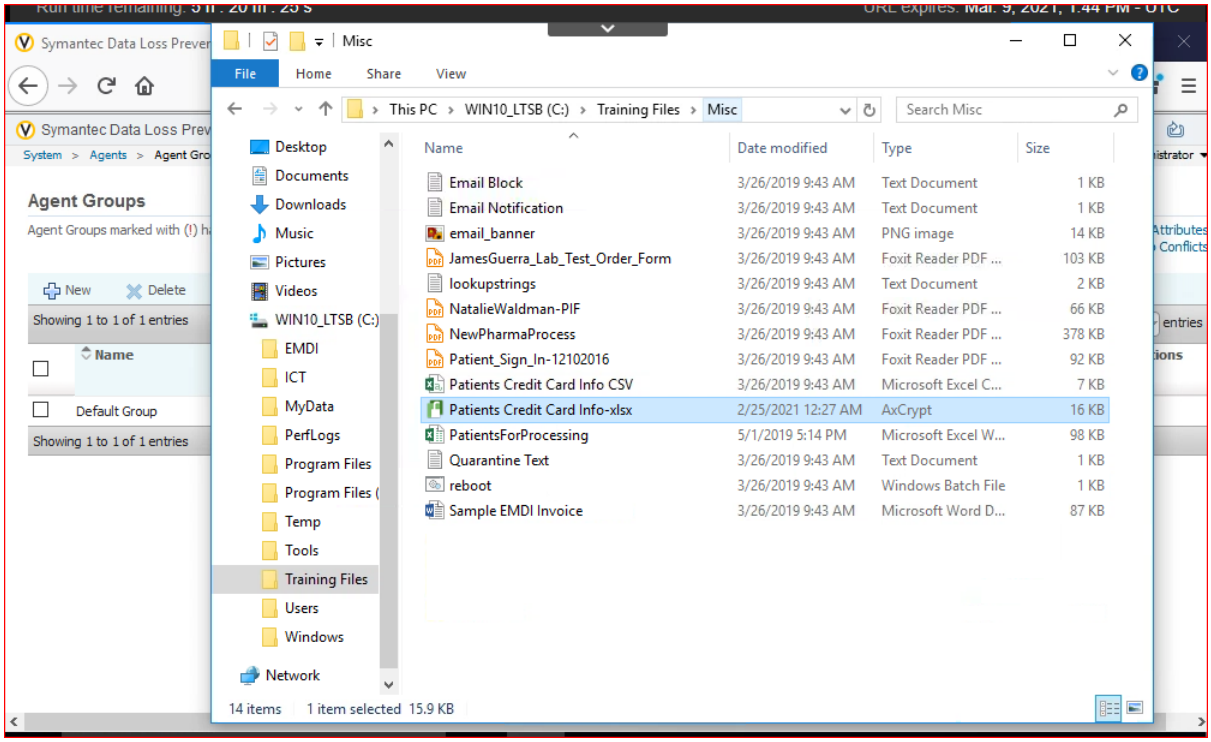


Setting the rules need to deselect everything and select application file access and select read option.

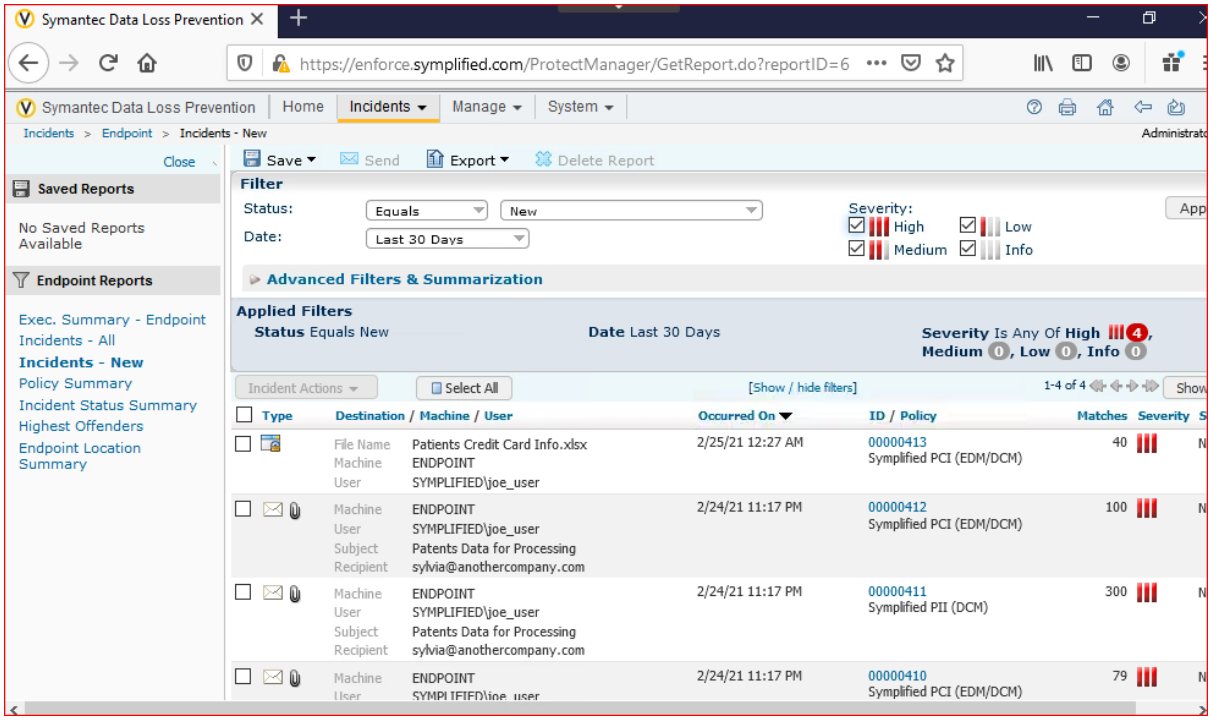
Vinay Kumar Reddy Donda dondavinayreddy@gmail.com



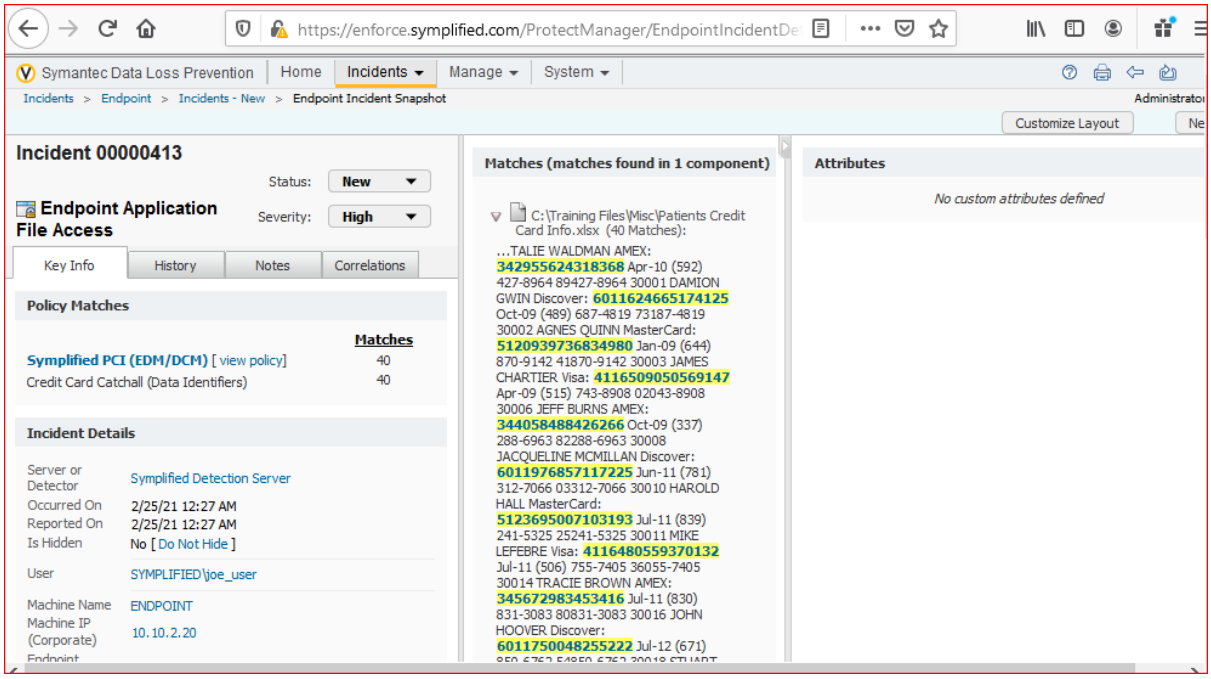
Adding the rules.



Displaying that patient credit card info is encrypted with ACRYPT app.



When encrypted an incident is raised at the endpoint

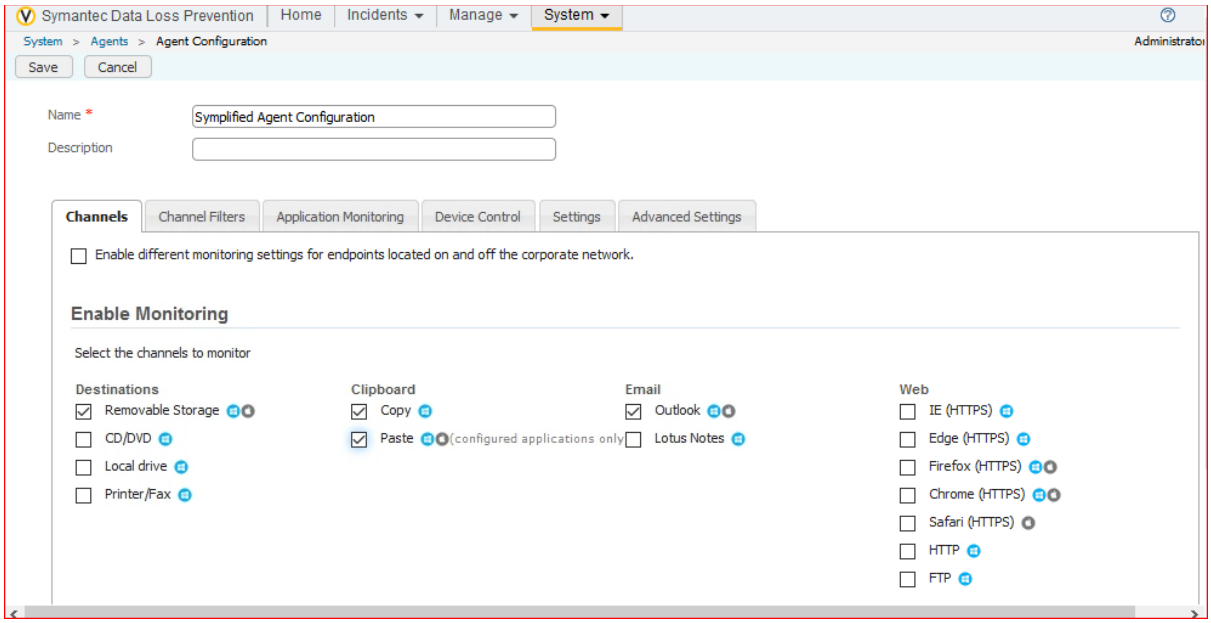


Incident is defined as the Endpoint Application file Access.

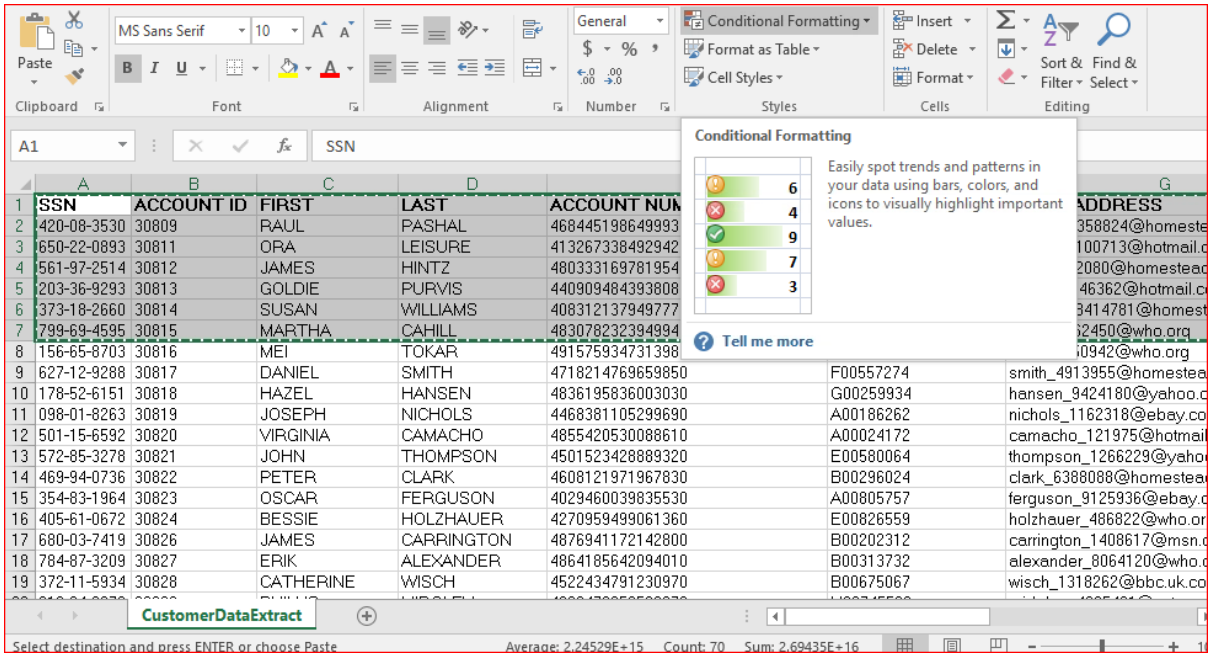
Exercise 5:

Monitor end point activity copy/paste

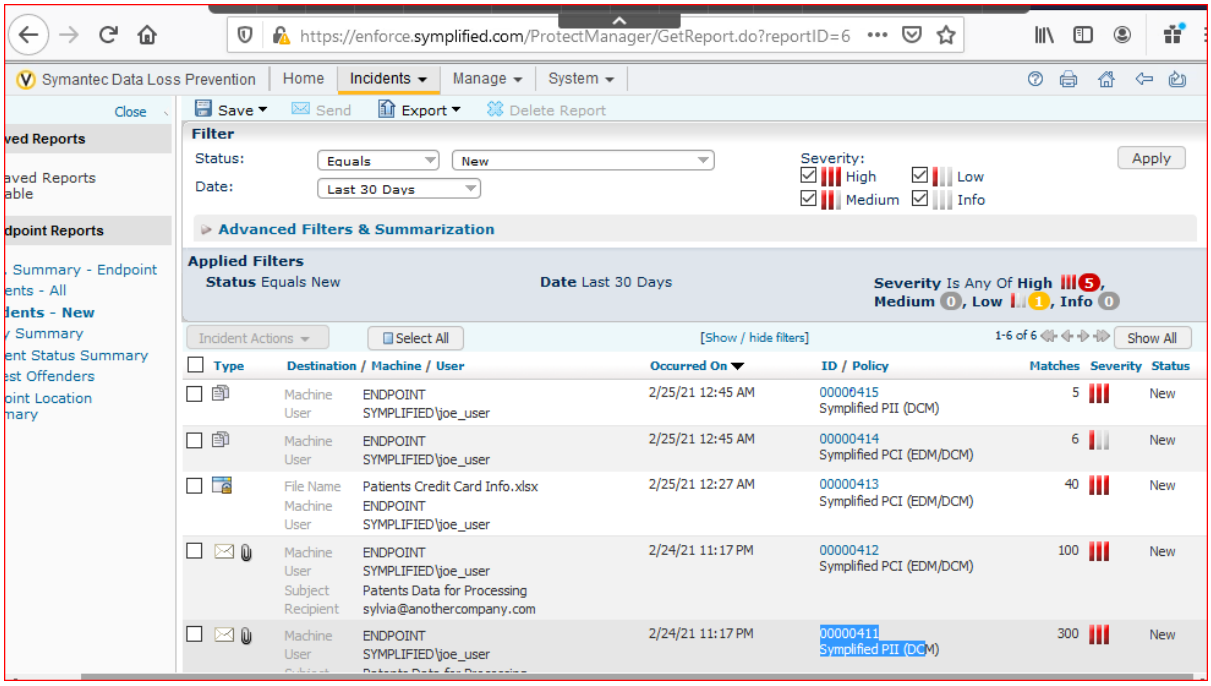
Malicious intruders inside the organization can leak the information and they try to copy/paste the information We will now see how this endpoint detects the copy paste operation.



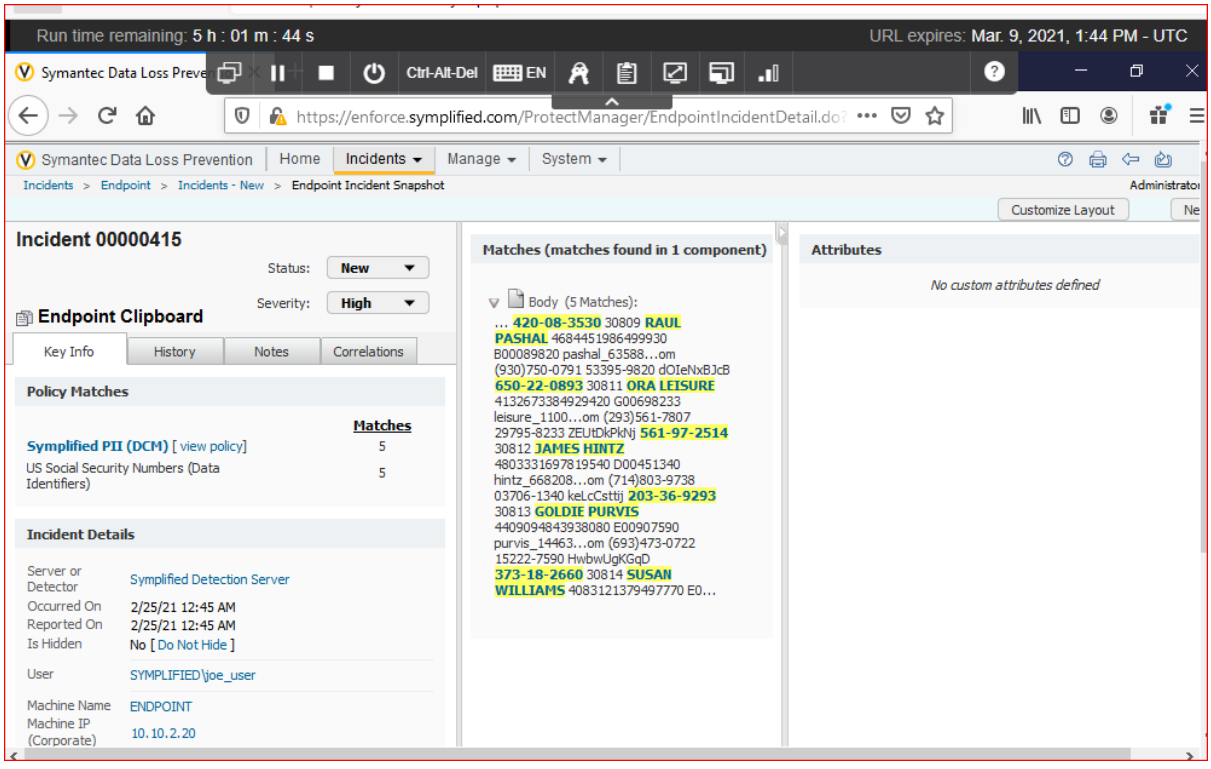
Adding the rule for copy and paste.



Copying the data



I tried copying the data twice so two incidents raised at the endpoint



The raised incident is described as the endpoint clipboard.

Section 4 or lab 4:

Educating users to Adopt data Protection practices.

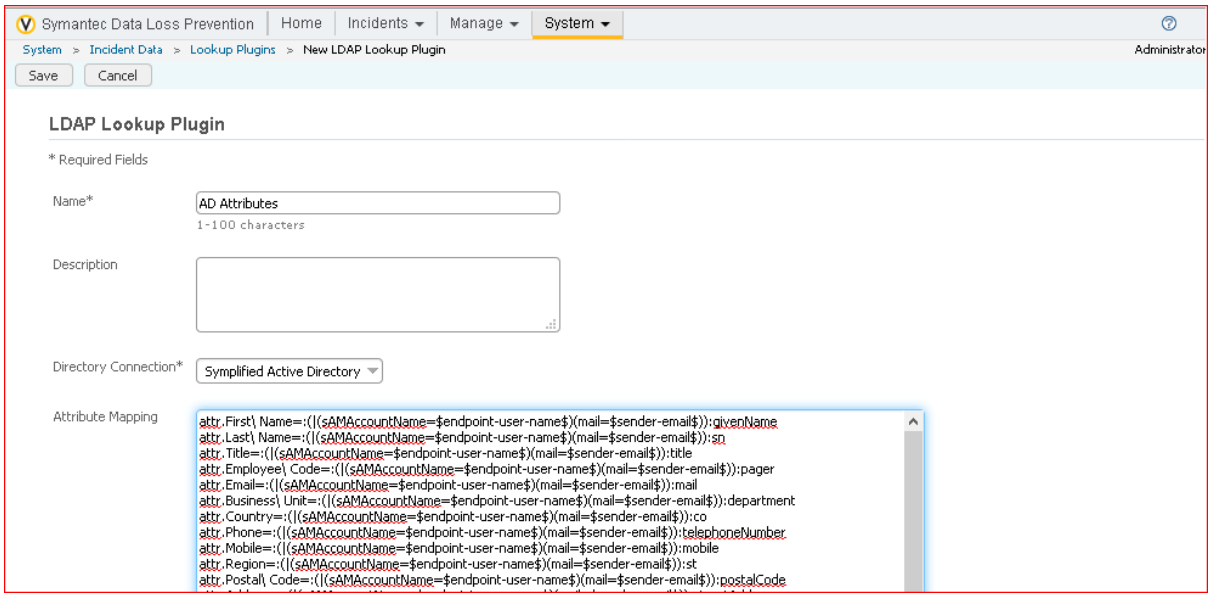
Not all the time data loss can be intentional sometimes it can be due to lack of awareness or carelessness so they should be educated for stopping the sensitive data loss. It basically describes about what actions are allowed and disallowed.

In this lab we will be configuring the policies such that notifications will be raised like you violated this policy. It basically gives us the policy and we

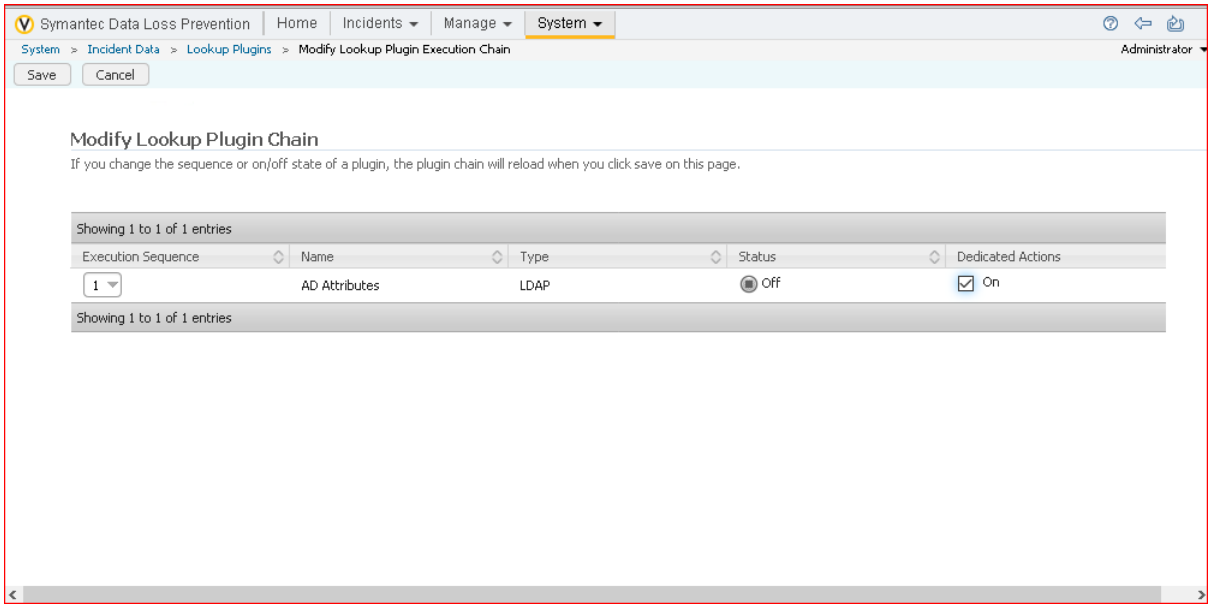
Exercise 1:

Configure the Active directory look up plugin:

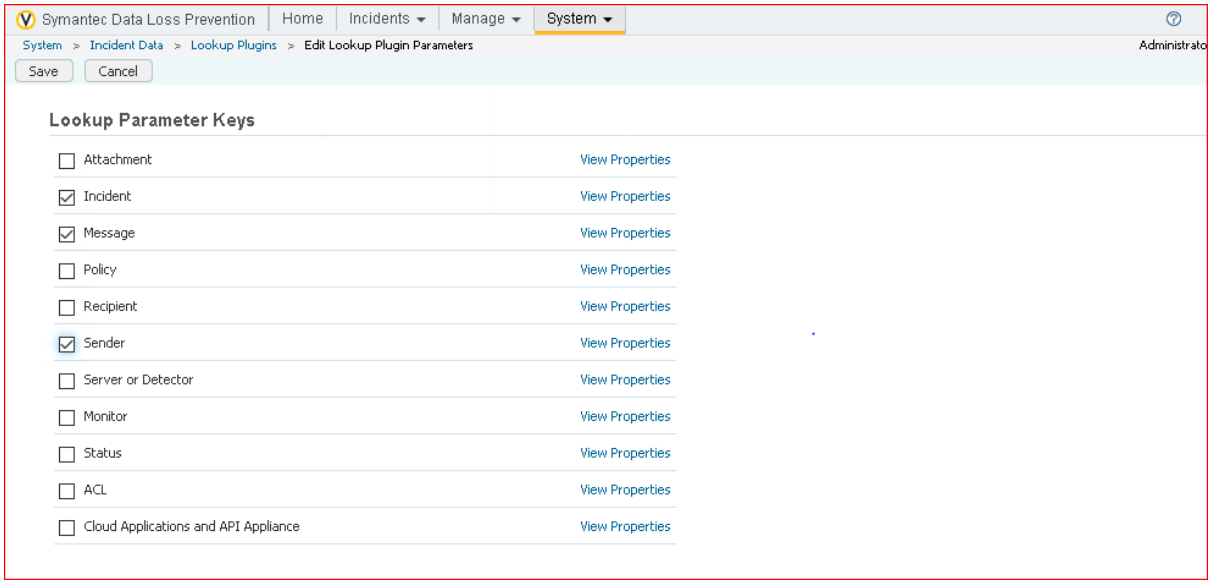
Lookup plugins enable the DLP to import the data from the external sources and import into the incidents. Symplified would like to import the additional contextual data from the active directory into the new incidents that are created. This will allow the Enforce server to send notifications to the user and their manager automatically.



Adding the plugin

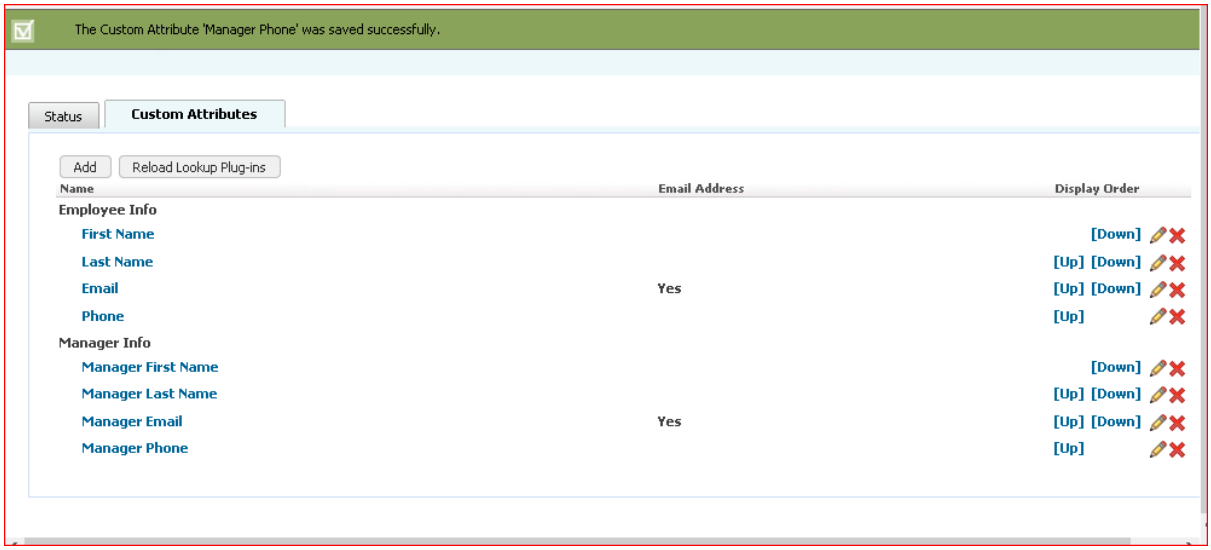


We need to on the dedication actions.



We need to enable the incident,message and sender.

Added the custom attributes.



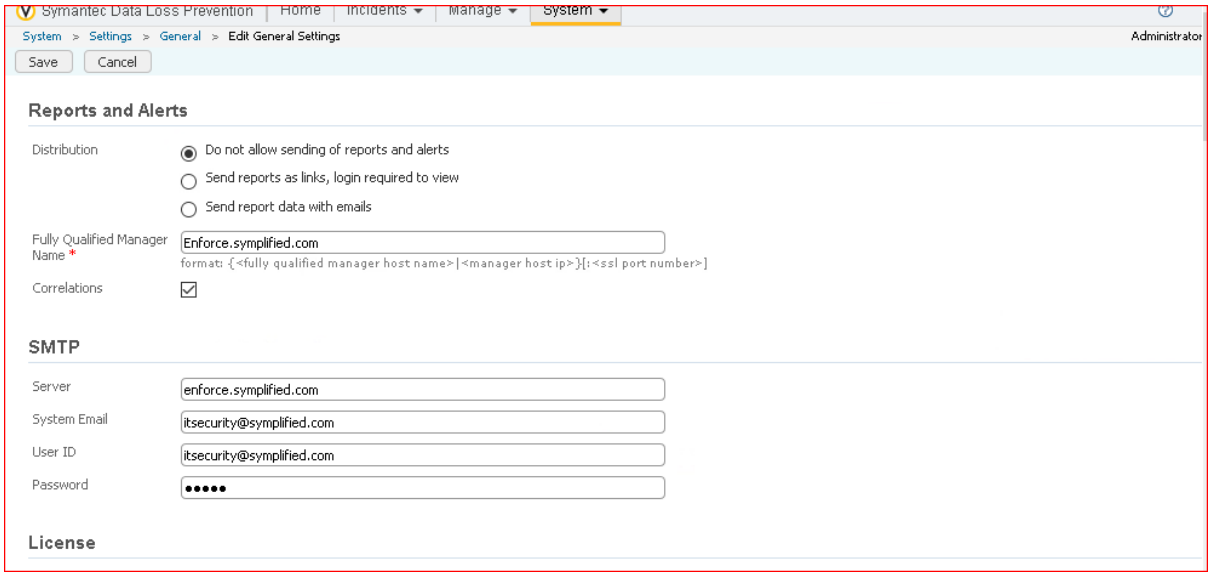
All the custom attributes were added.

Exercise 2:

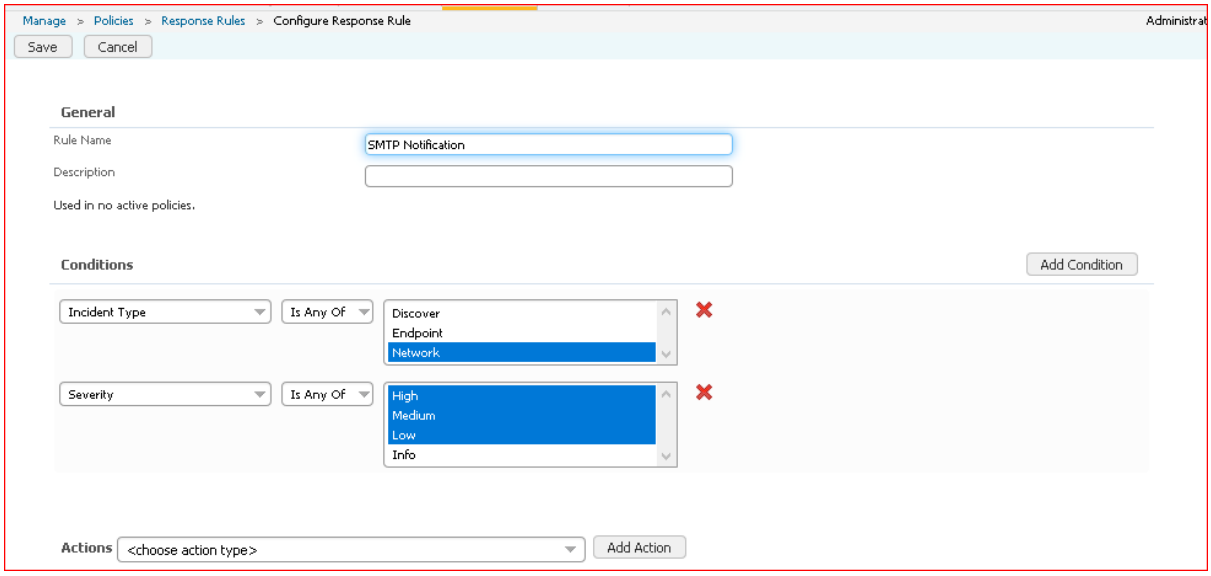
Configure Email Notifications.

The name itself saying that when a user is violating the policy while using the outlook the user will get the notification to the email about the voilation and also along with the user, the manager , and the infosec team will be receiving the notifications. In this lab we will discuss about how it is going to work.

Note: This is not the on screen notification or pop up notification. It sends the notification to the email.

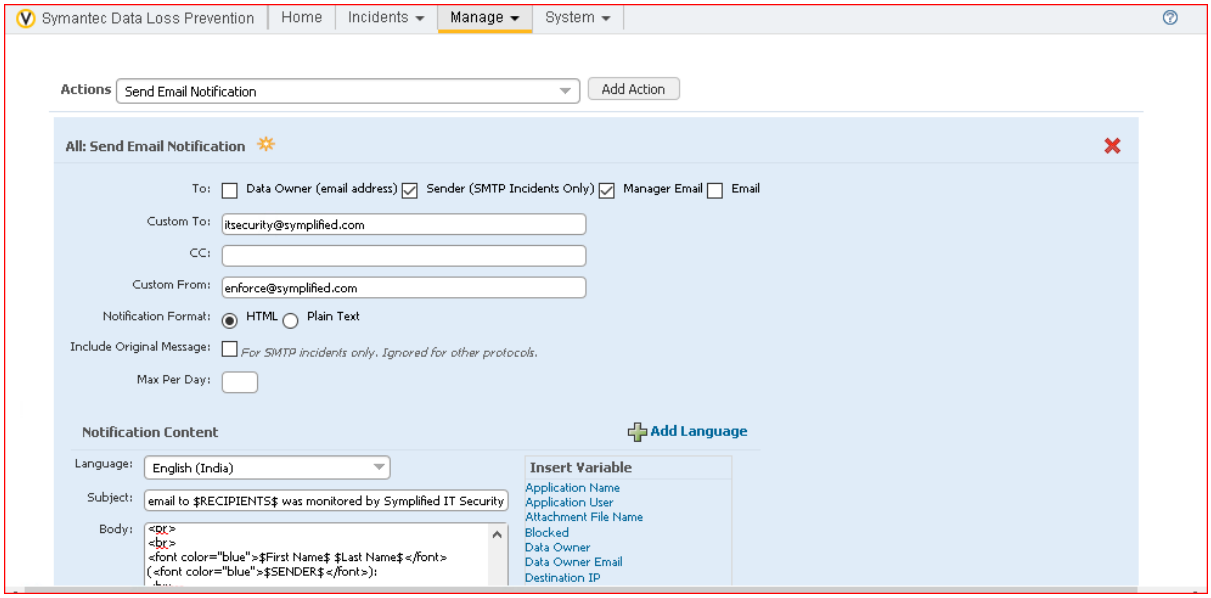


Setting the smtp rules.

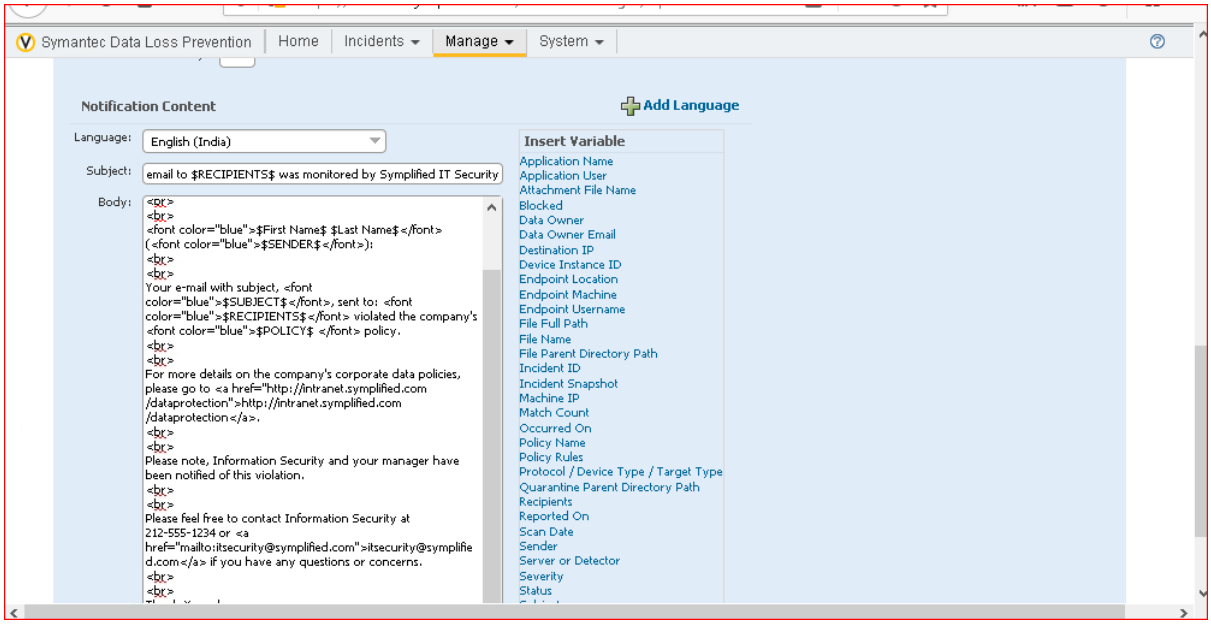


Creating the response rules.

Vinay Kumar Reddy Donda dondavinayreddy@gmail.com

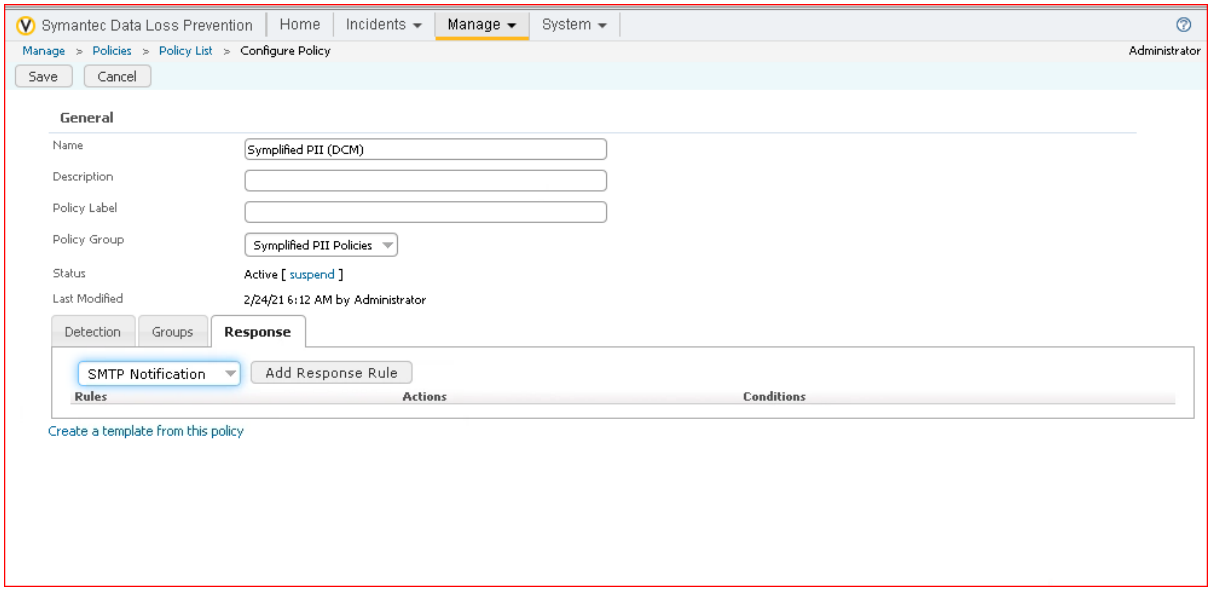


Adding the actions

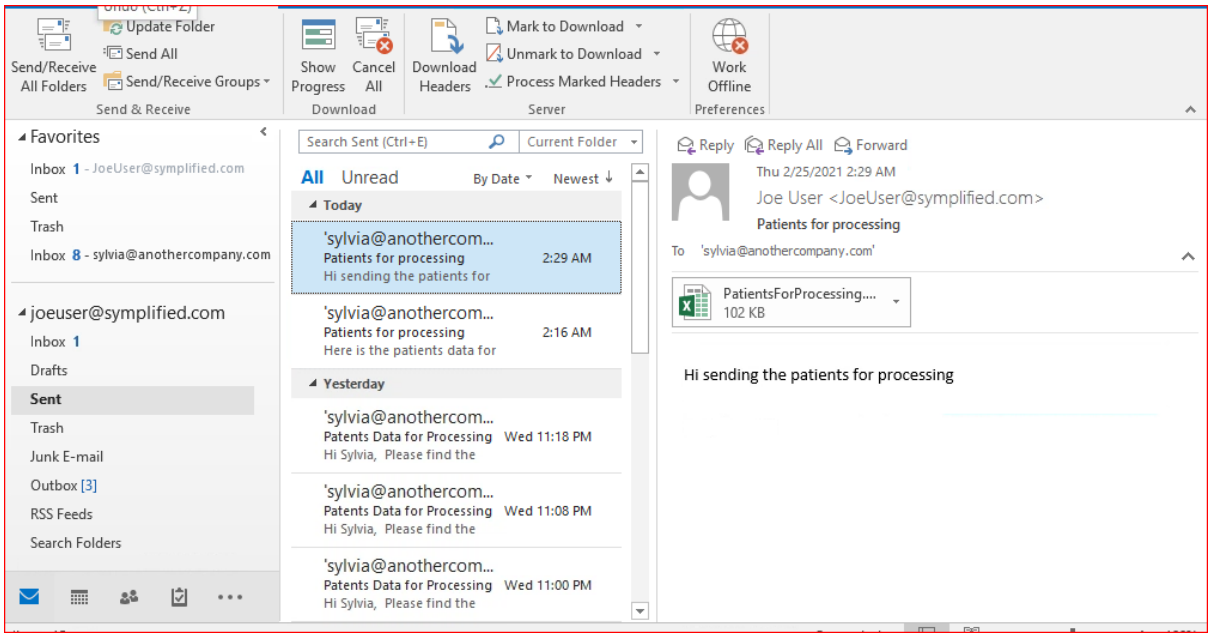


Adding the actions

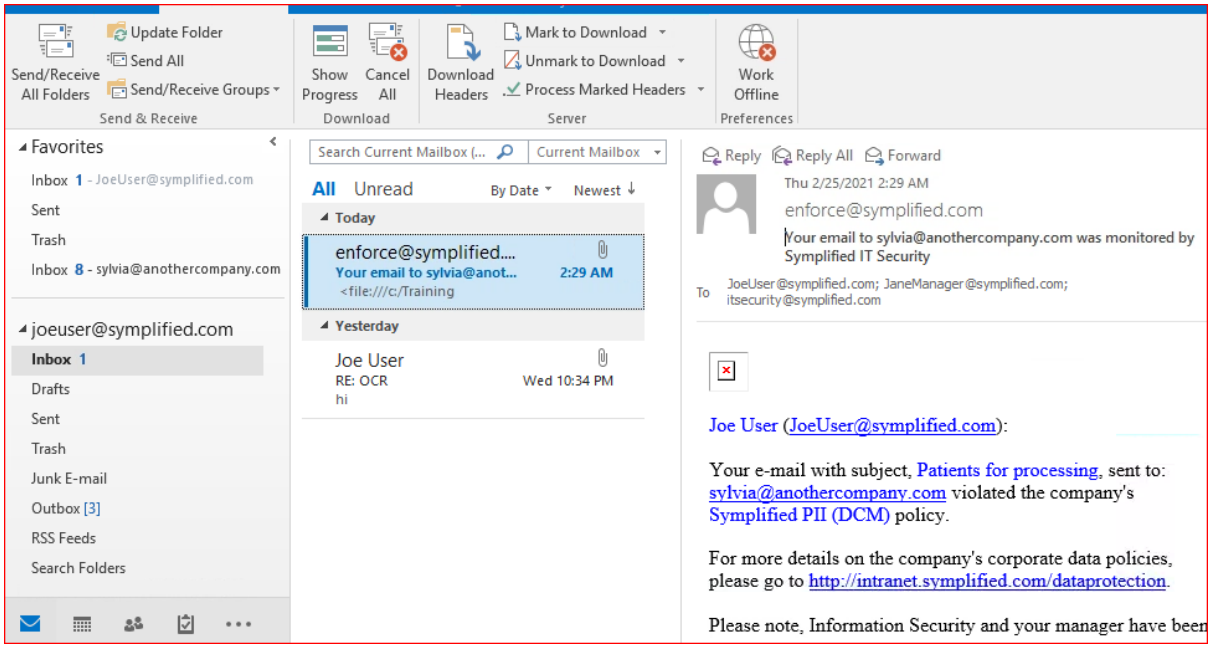
Vinay Kumar Reddy Donda dondavinayreddy@gmail.com



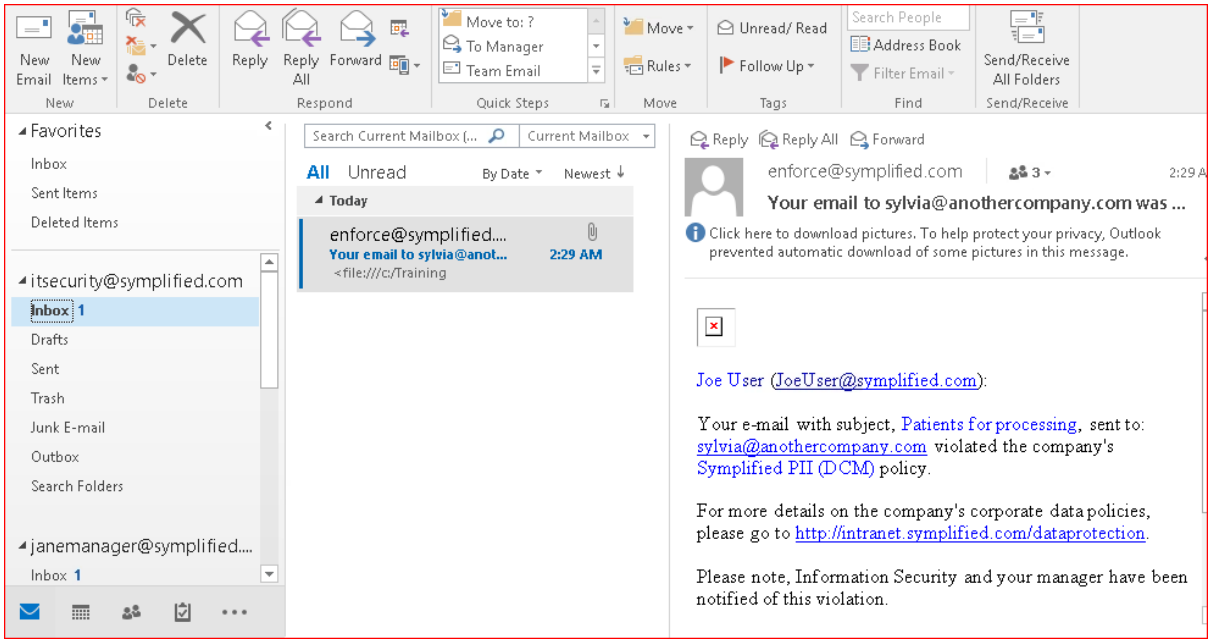
Adding the notification



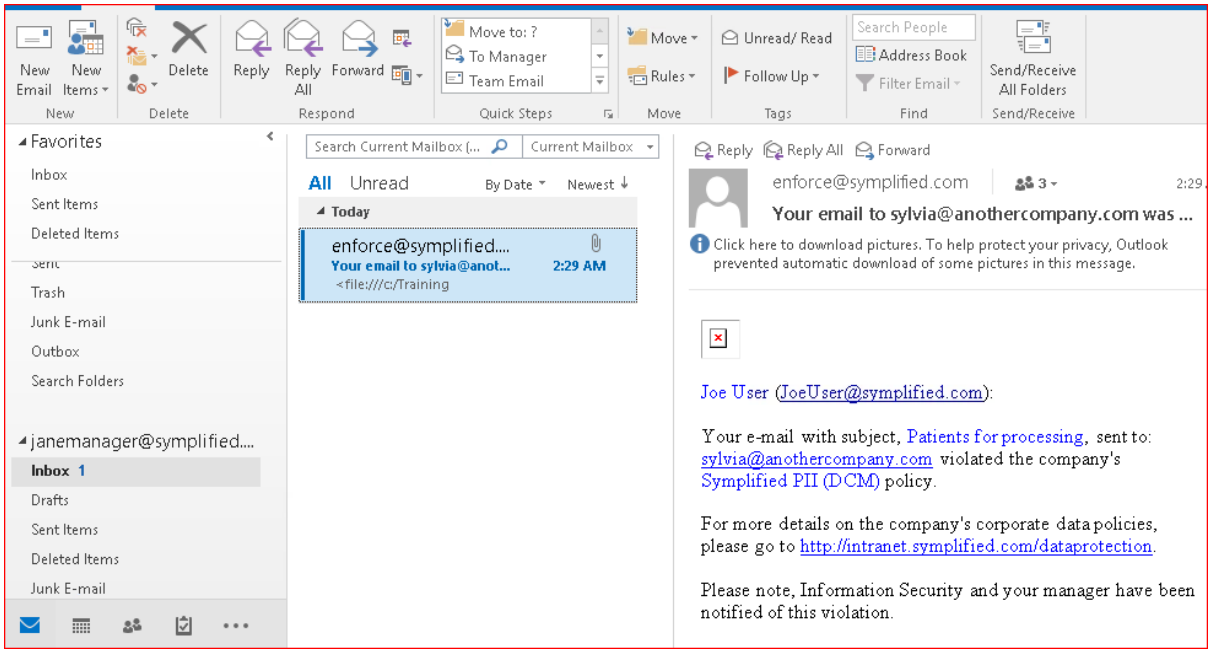
Email from joe is sent to the sylivia



This telling that jeo got a mail like he violated the companies policy.



This describes that itsecurity department also got notification about joe violated the policy.



This described that jane who is manager also received about joe violated the policy.

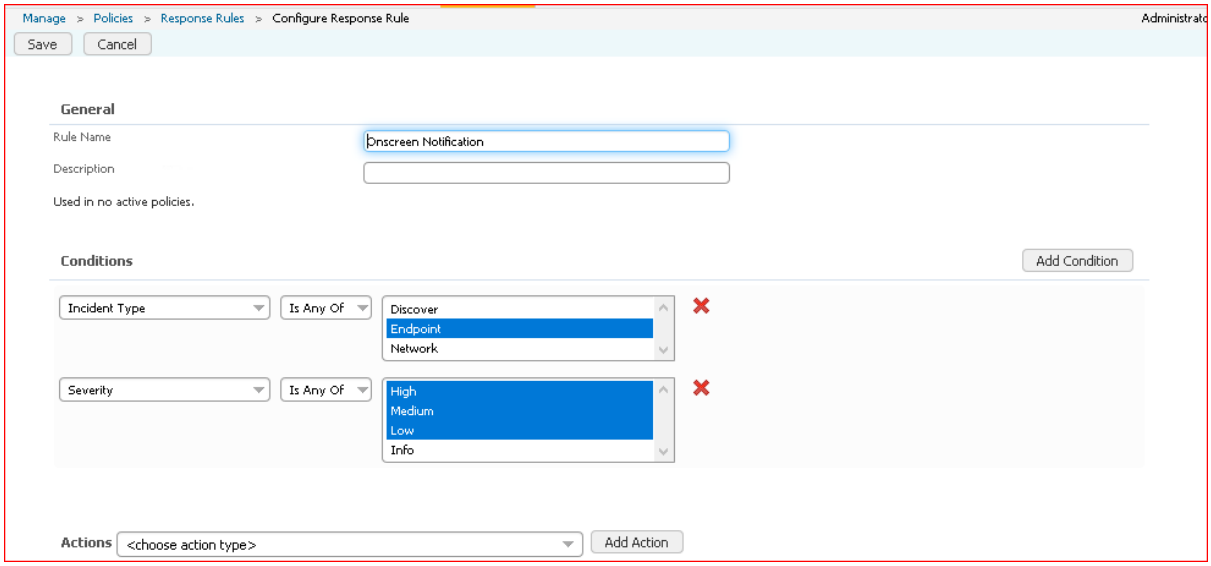
In this way email notifications will be sent if the policy is violated.

Vinay Kumar Reddy Donda dondavinayreddy@gmail.com

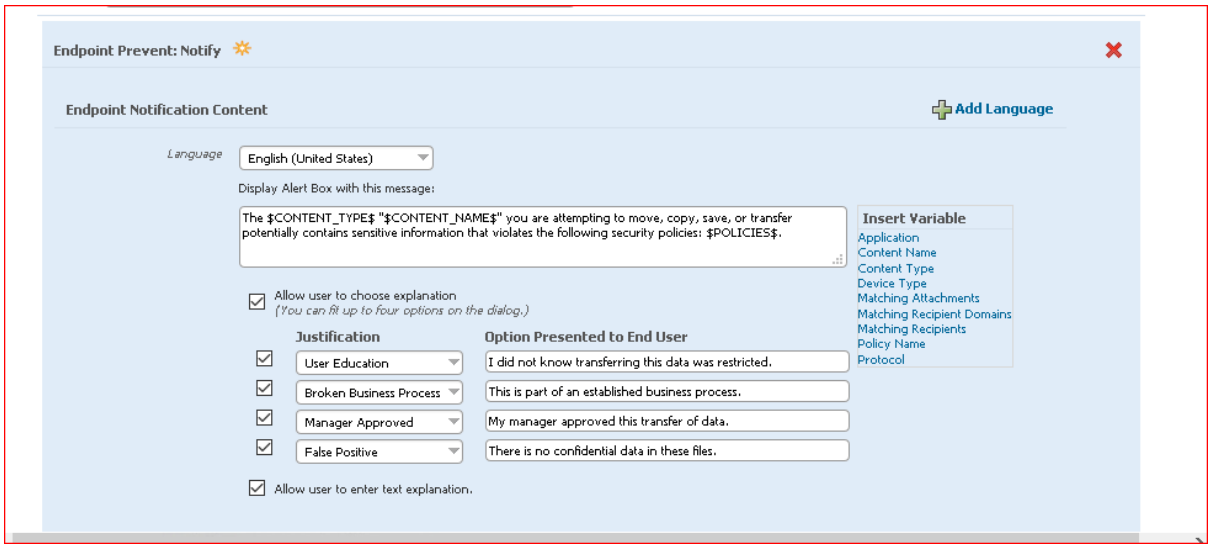
Exercise 3:

Configure the on screen notifications.

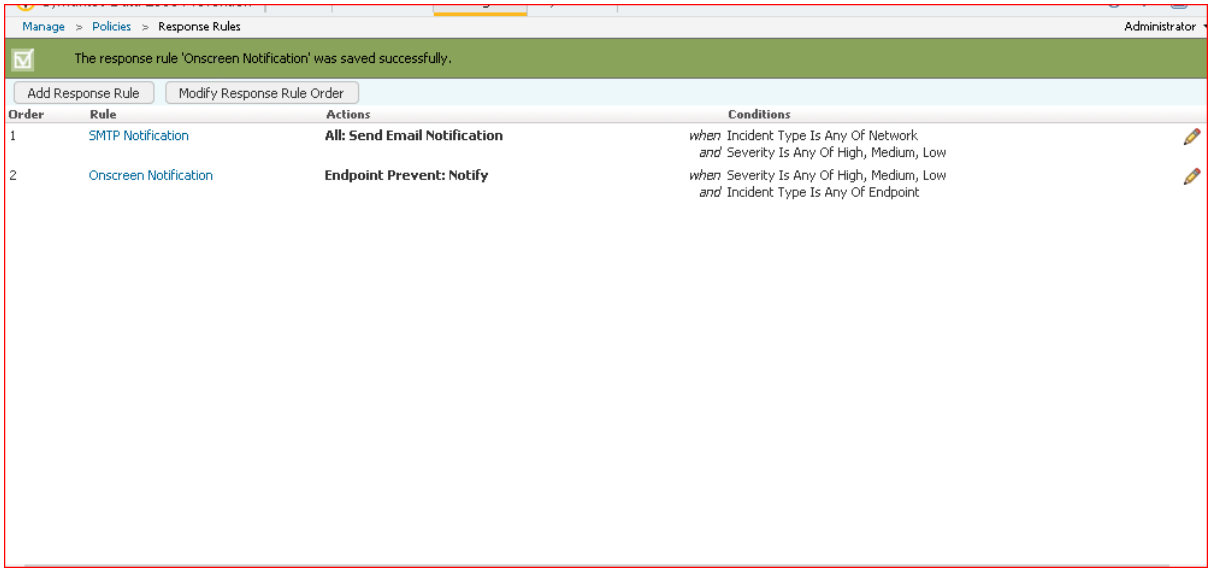
This basically notifies about the sensitive data mis usage through direct pop up notifications.



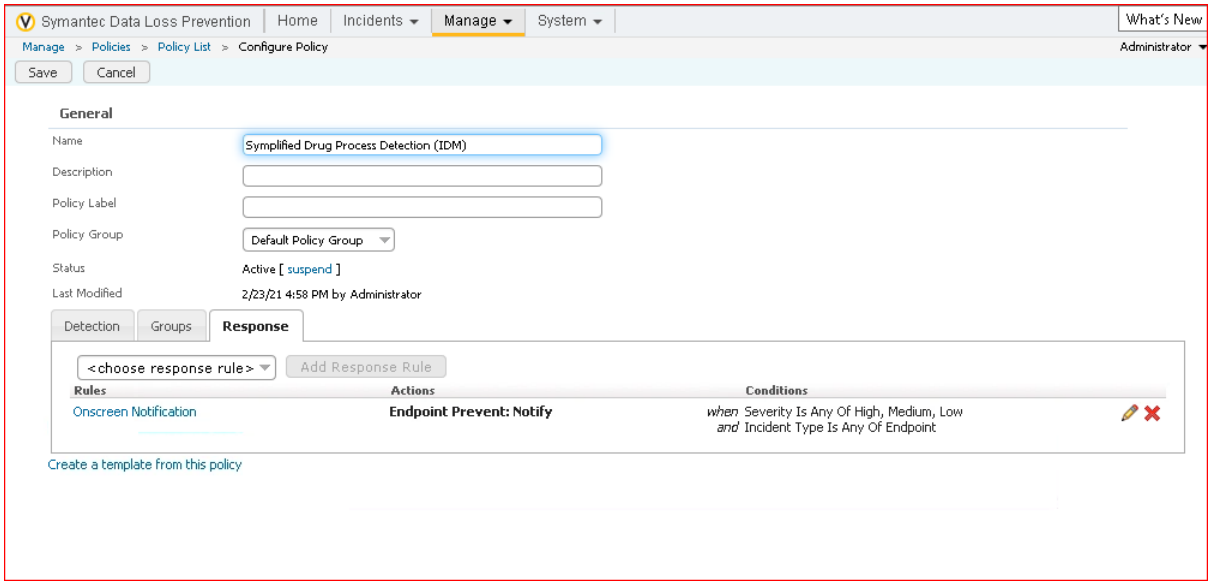
Configuring the response rules.



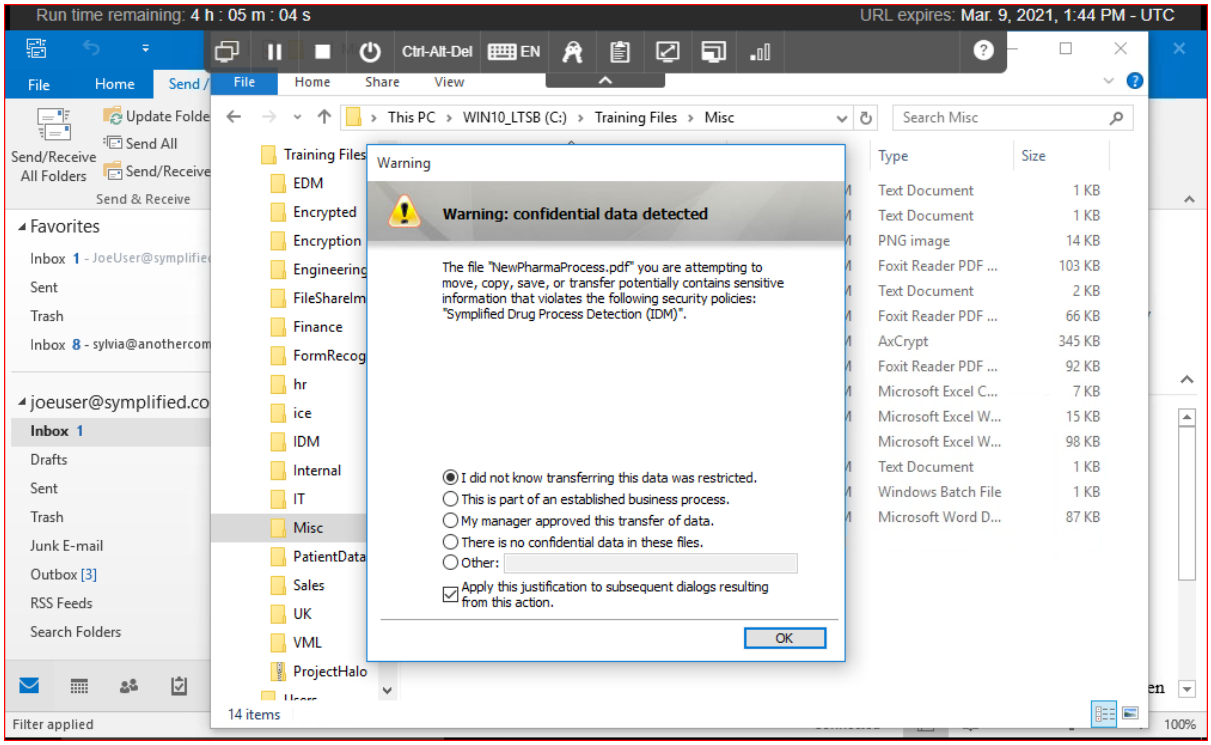
What should be notified is added here.



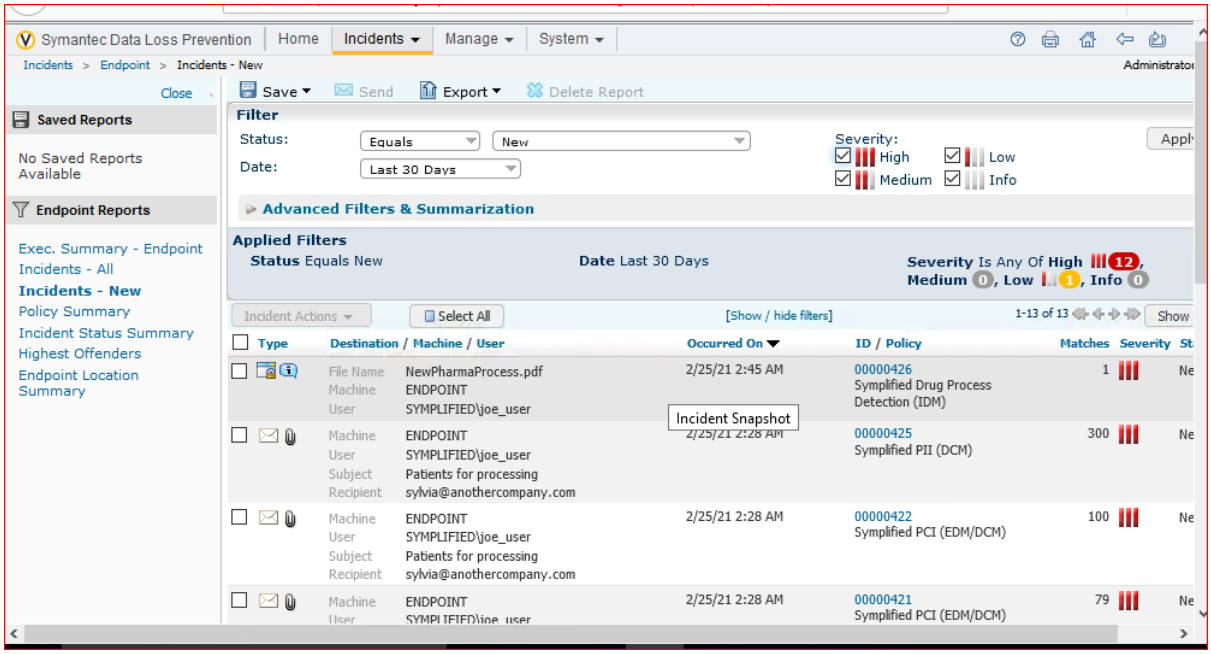
Overview of the response rules.



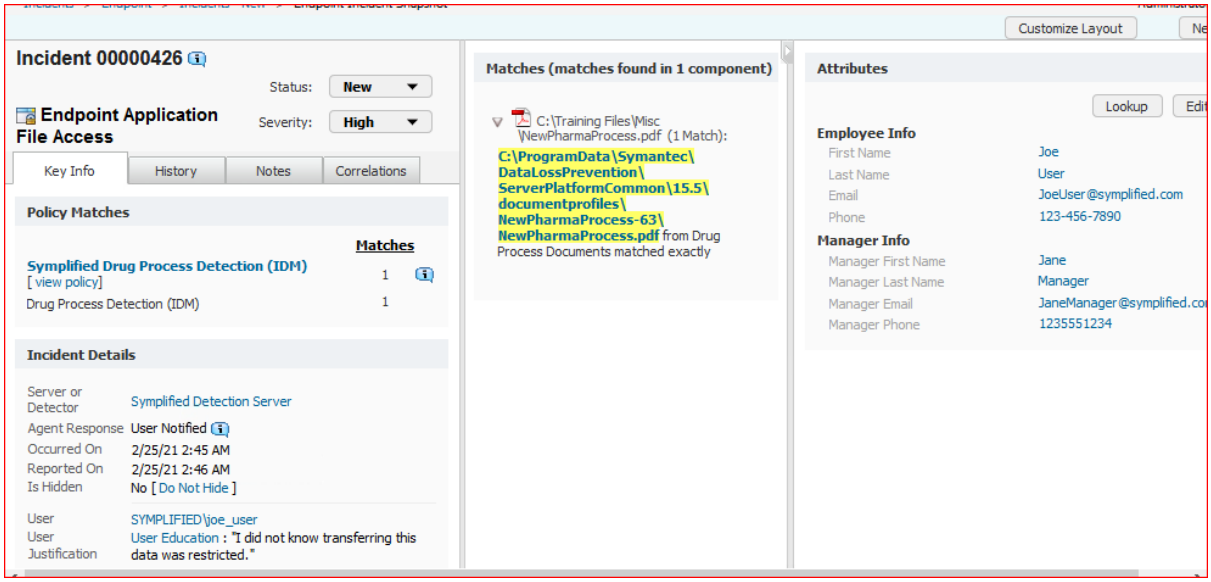
Added the onscreen notification.



When iam trying to encrypt the data its giving the notification.



We can clearly see that incident at the endpoint is captured.



We can clearly see that in the incident details its showing the user was notified while encrypting the data and along with that its saying that user was responded like “I did not know tranfering this data was restricted”

Lab 5:

Preventing unauthorized exposure of confidential data.

There are no of tools In order to prevent the sensitive data to be leaked.

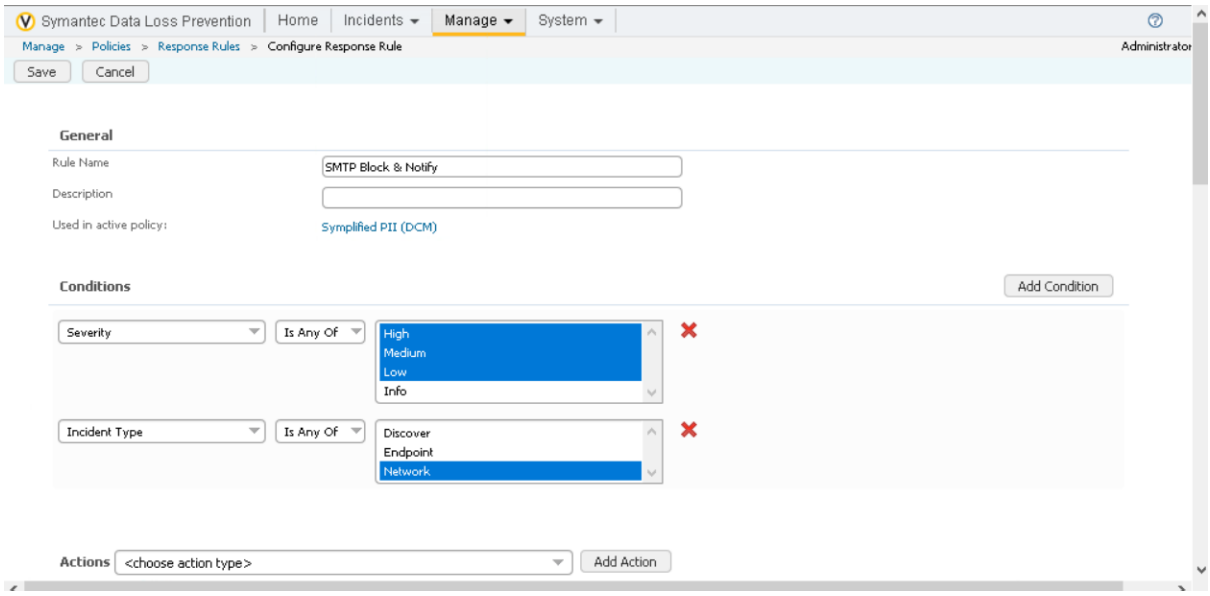
In this lab we will configure the appropriate responses to policies violations, including blocking , quarantaine and user notification. Also we gonna detect some of the advanced detection techniques like OCR that can find the sensitive data that has been converted to an image. Main concentration in on the data at rest even before becoming into data in motion.

Exercise 1:

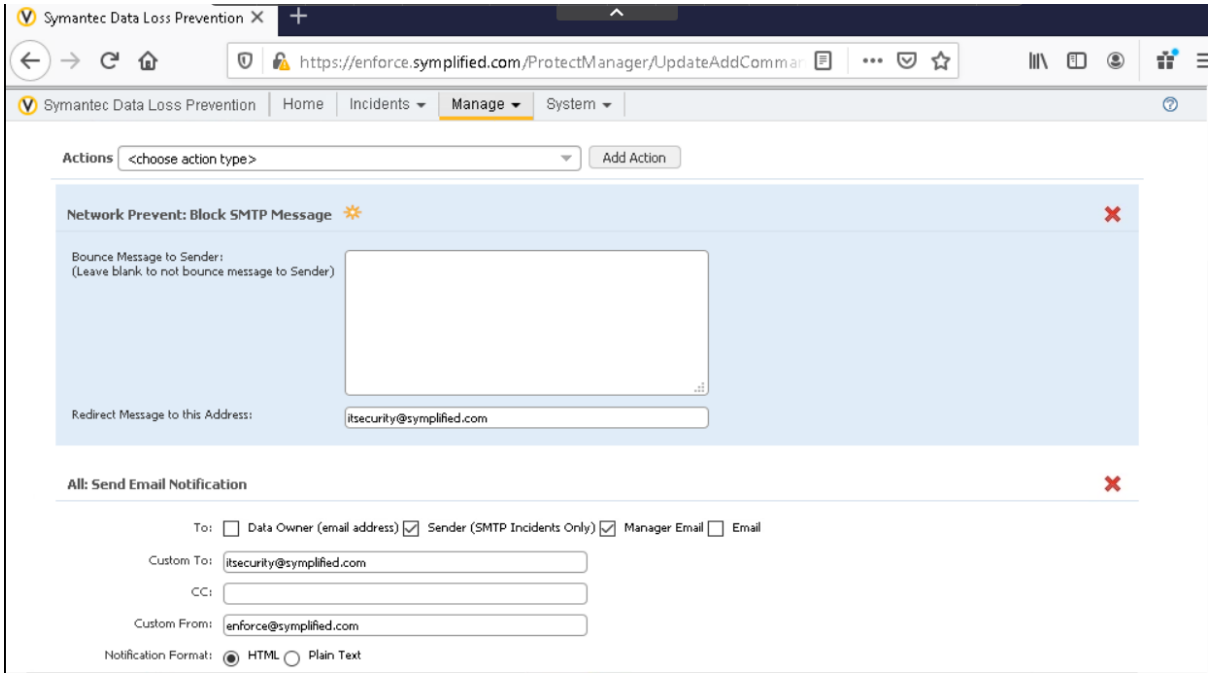
Configure SMTP blocking.

Till now we seen notifications to the email, pop-up notifications when the policy is violated but in this we will try to block the data from being sending if there is any policy violated immediately the data will be blocked and it won't send to the recipient.

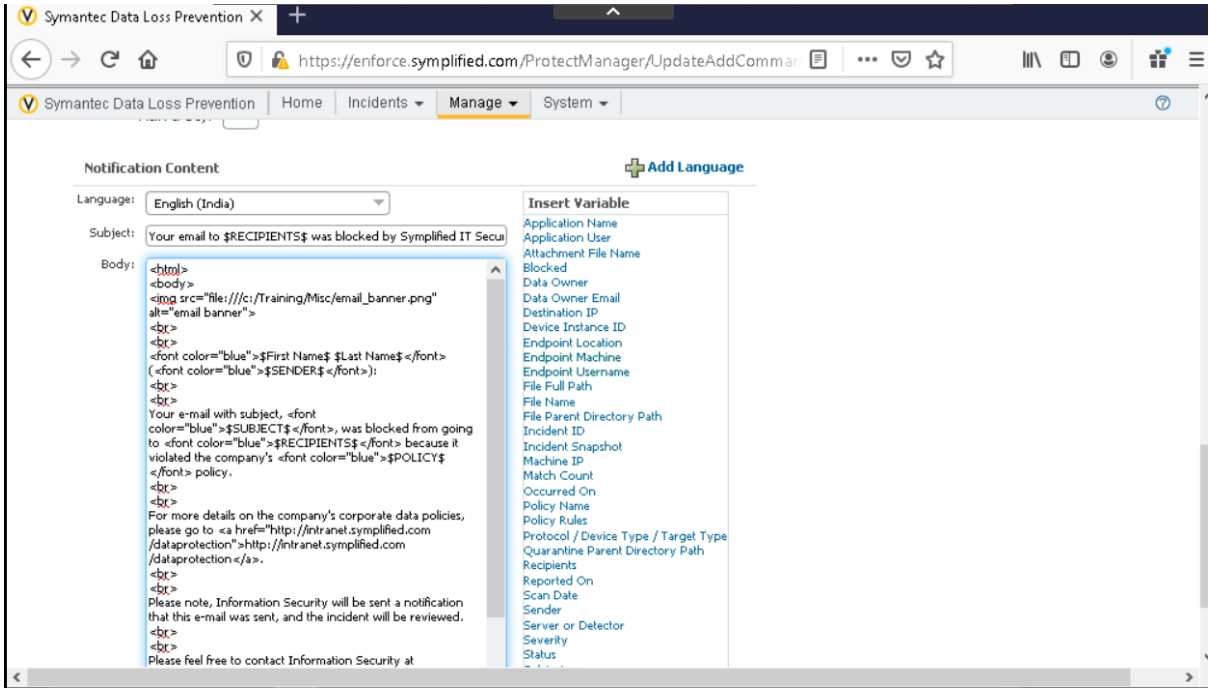
In this lab we will configure the smtp blocking i.e., when an sensitive data is sending through the mail it will be blocked before sending to the recipient.



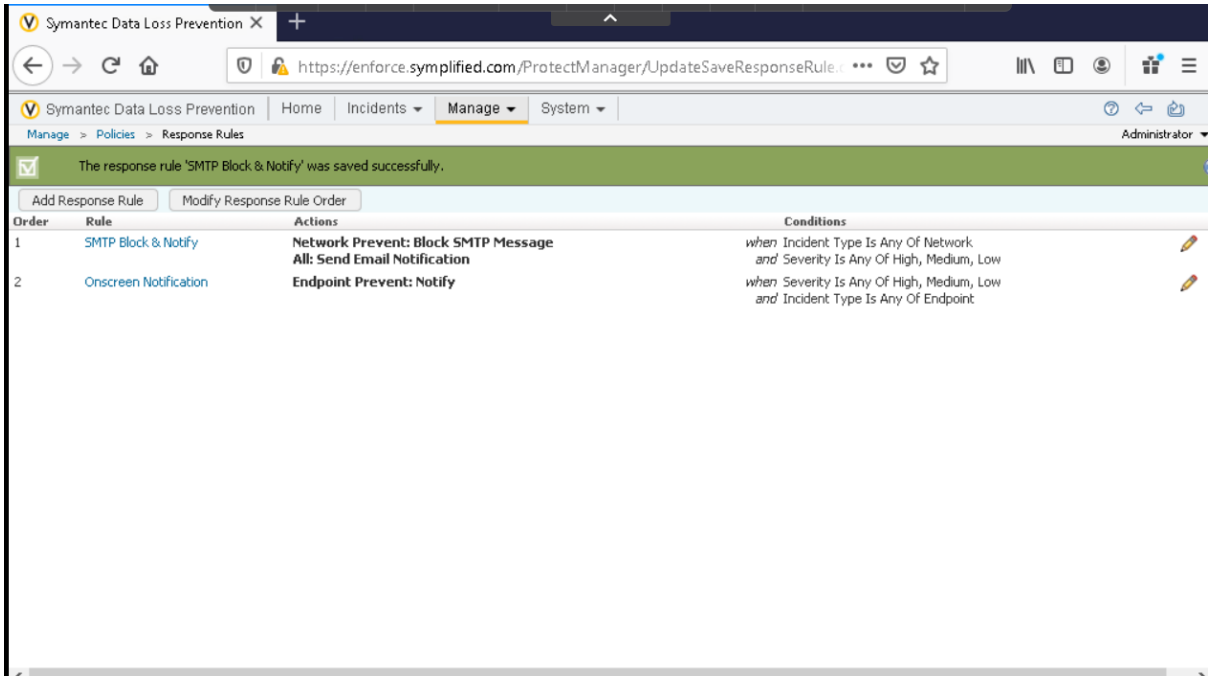
Configuring the response rules



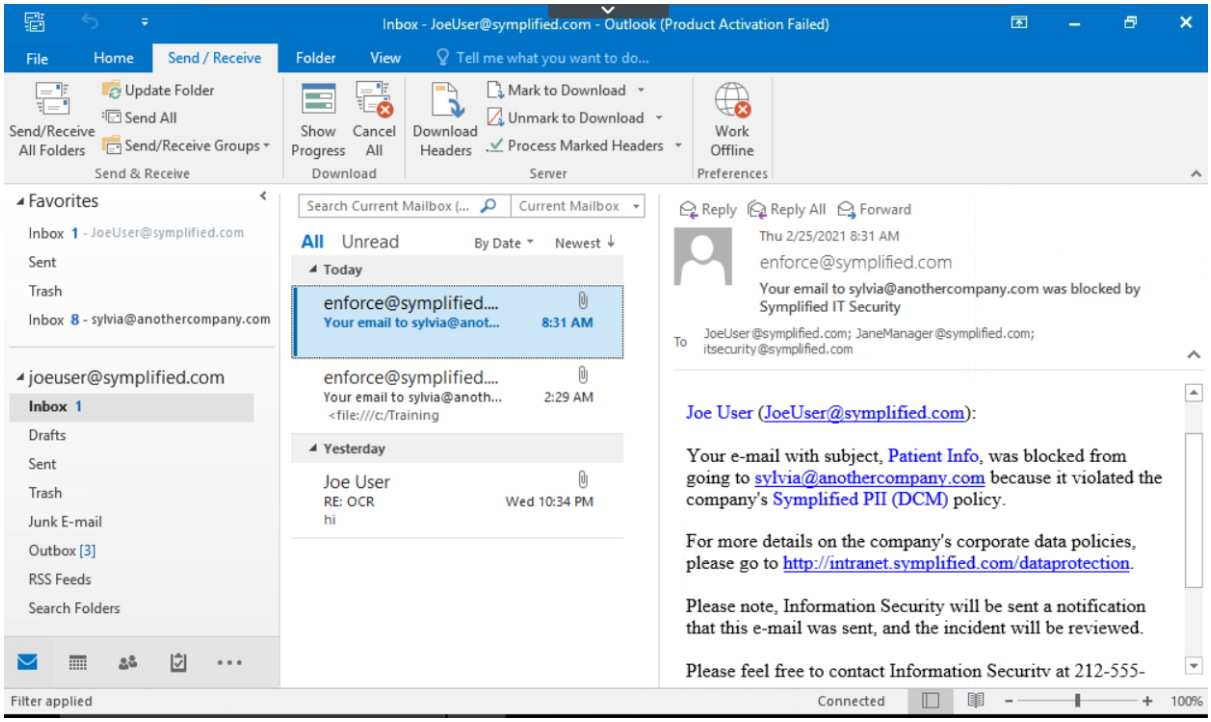
Configuring the response rules



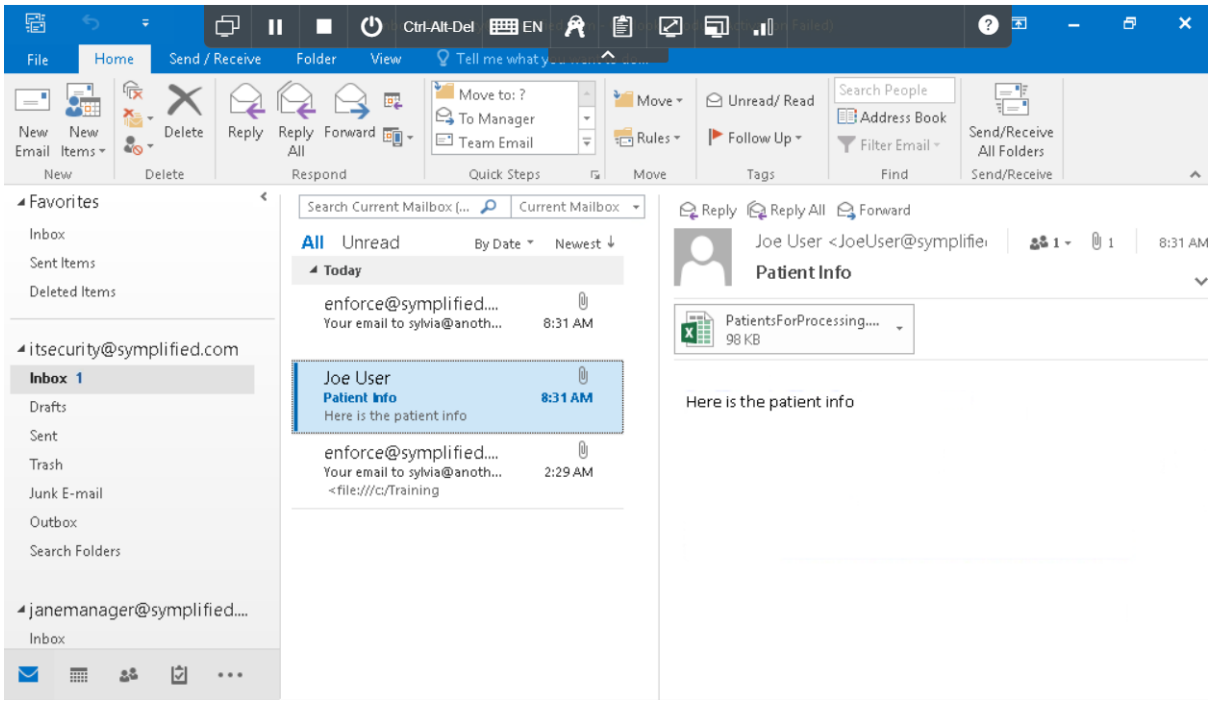
Configuring the response rules.



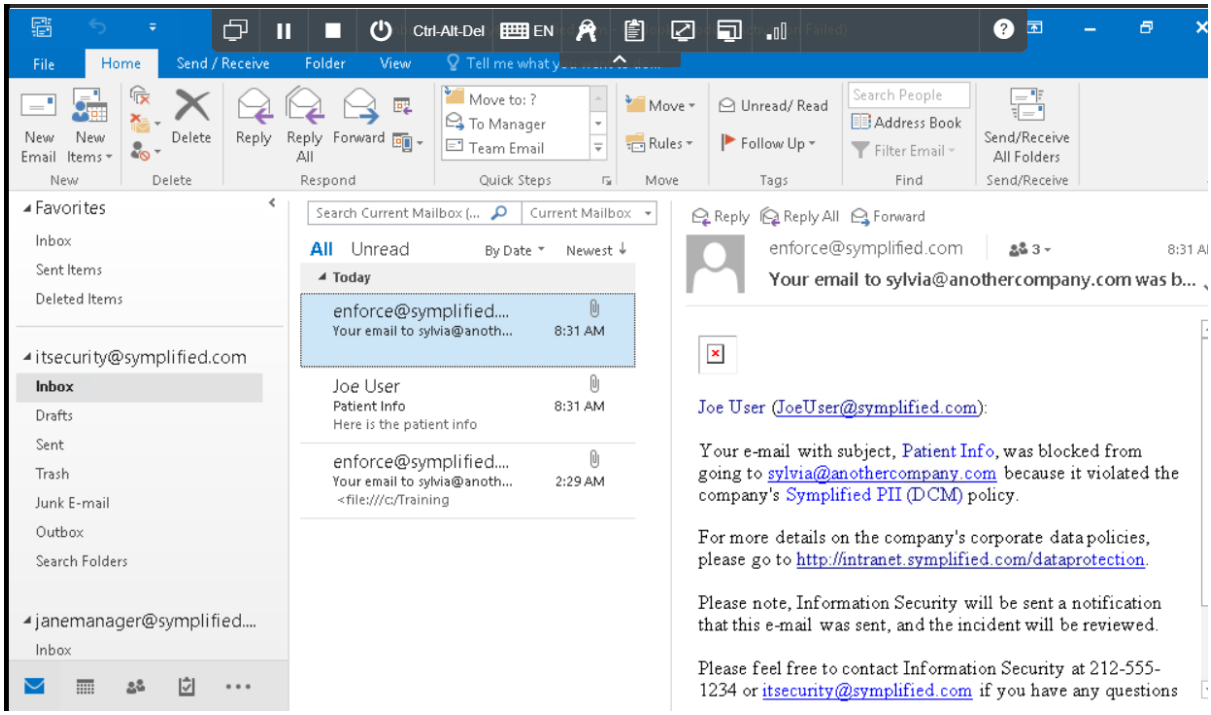
Proof that response rule is added.



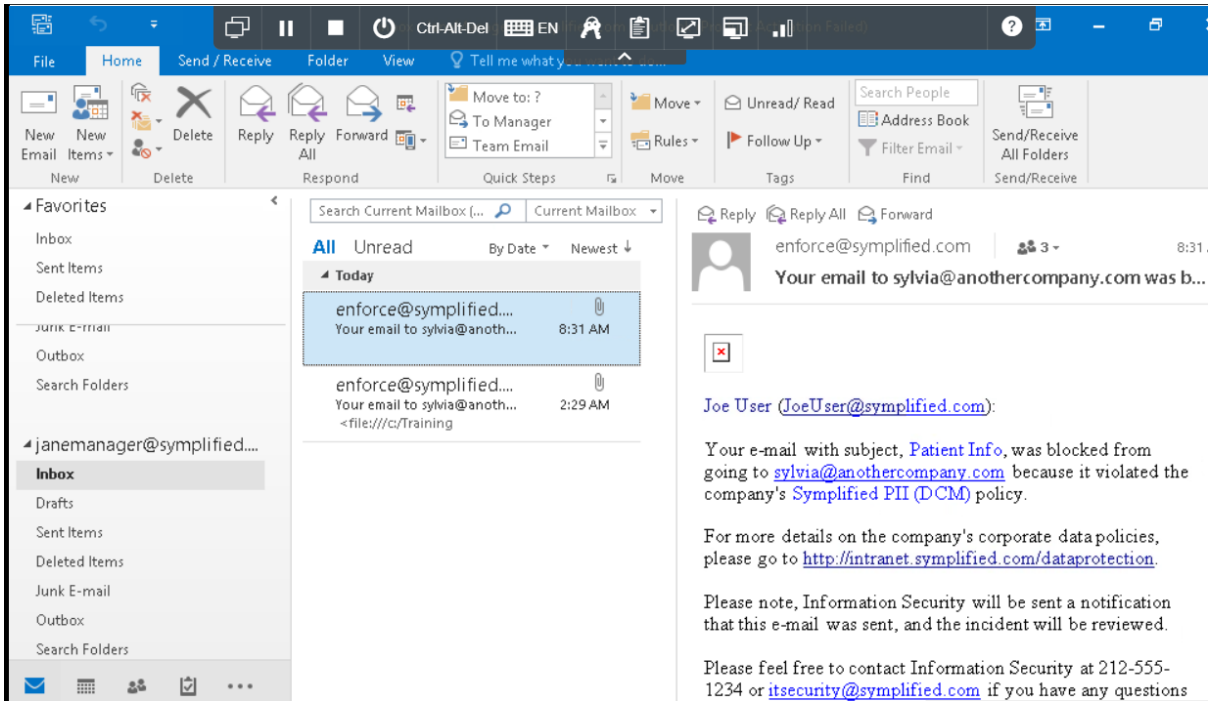
When iam trying to send the mail from joe to sylivia its clearly saying that it was blocked.



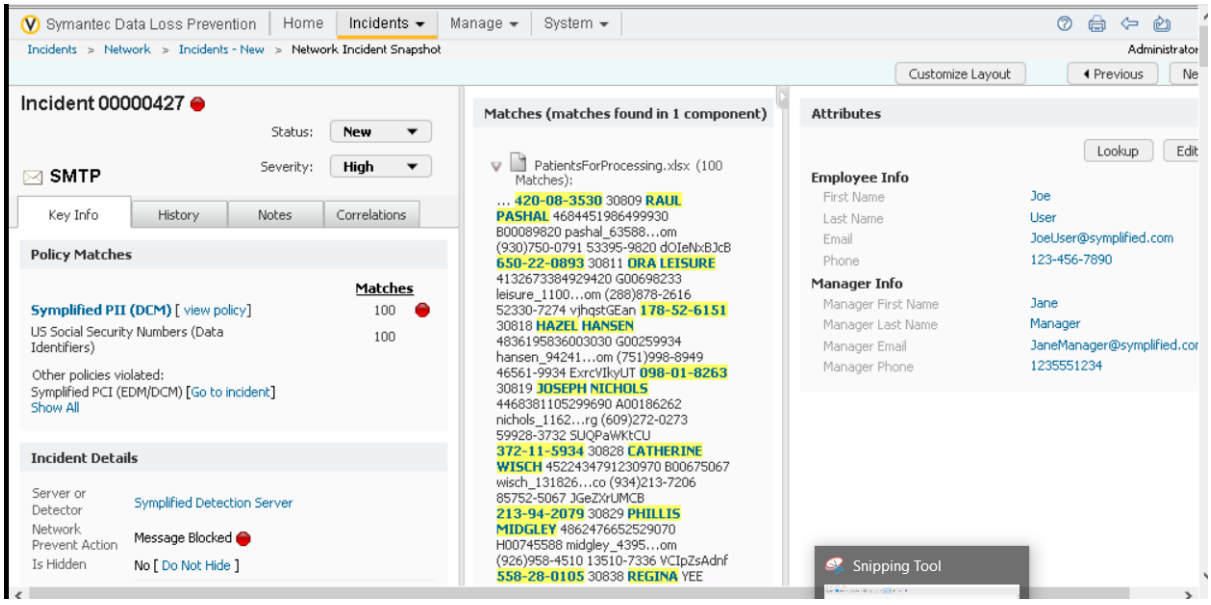
Here is the proof like it security department received the blocked mail



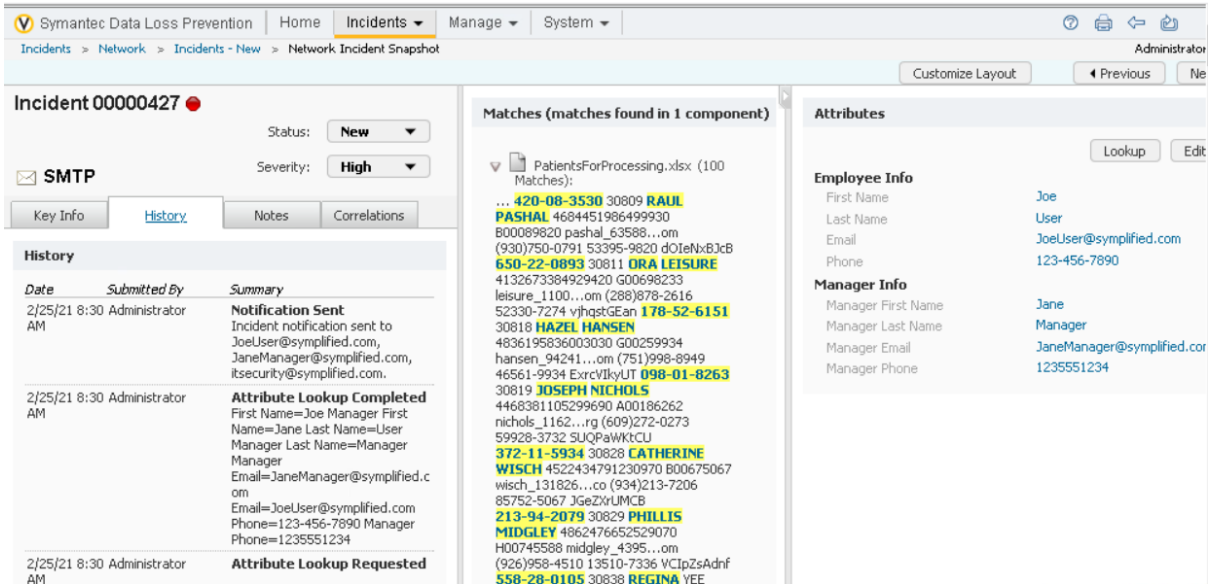
Here is the proof that itsecurity team also received the notification.



Here is the proof that jane manager also received the notification mail.



Here is the proof that the incident is raised in the network and red mark indicating that message is blocked.



History tab shows us the incident related to that which occurred earlier.

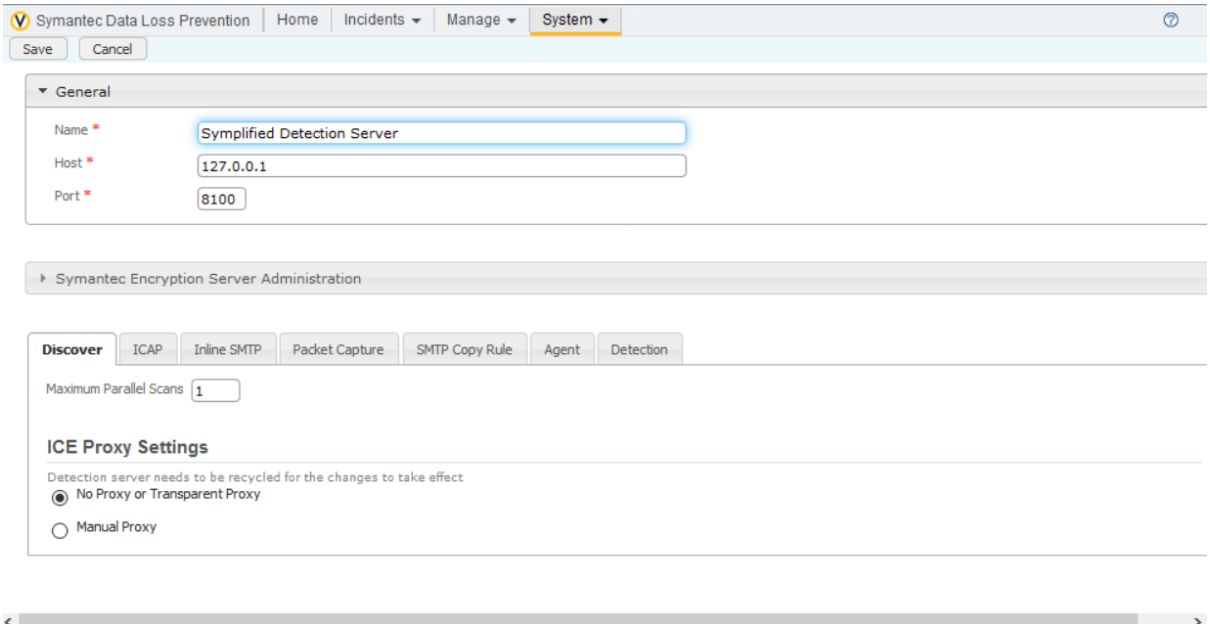
Vinay Kumar Reddy Donda dondavinayreddy@gmail.com

Exercise 2:

Testing Optical character recognition(OCR) and “HIPAA and HITECH (including PHI)” Policy.

Symplified is testing a new policy for its US offices along with an additional Symantec DLP feature. They have created a test policy called “HIPAA and HITECH(including PHI),” based on Symantec DLP policy template, that looks for combinations of medical keywords and USsocial security numbers. The simplified DLp administrators have also installed a Symantec DLP OCR server for testing and have configured one of their detection servers to send OCR-amenable iamges to the OCR server for text extraction. They are noew going to run a tes of this setup.

Note: Since this lab is associated with the OCR configuration as we are unable to create the OCR policy we cannot proceed with this exercise so iam skipping this part.

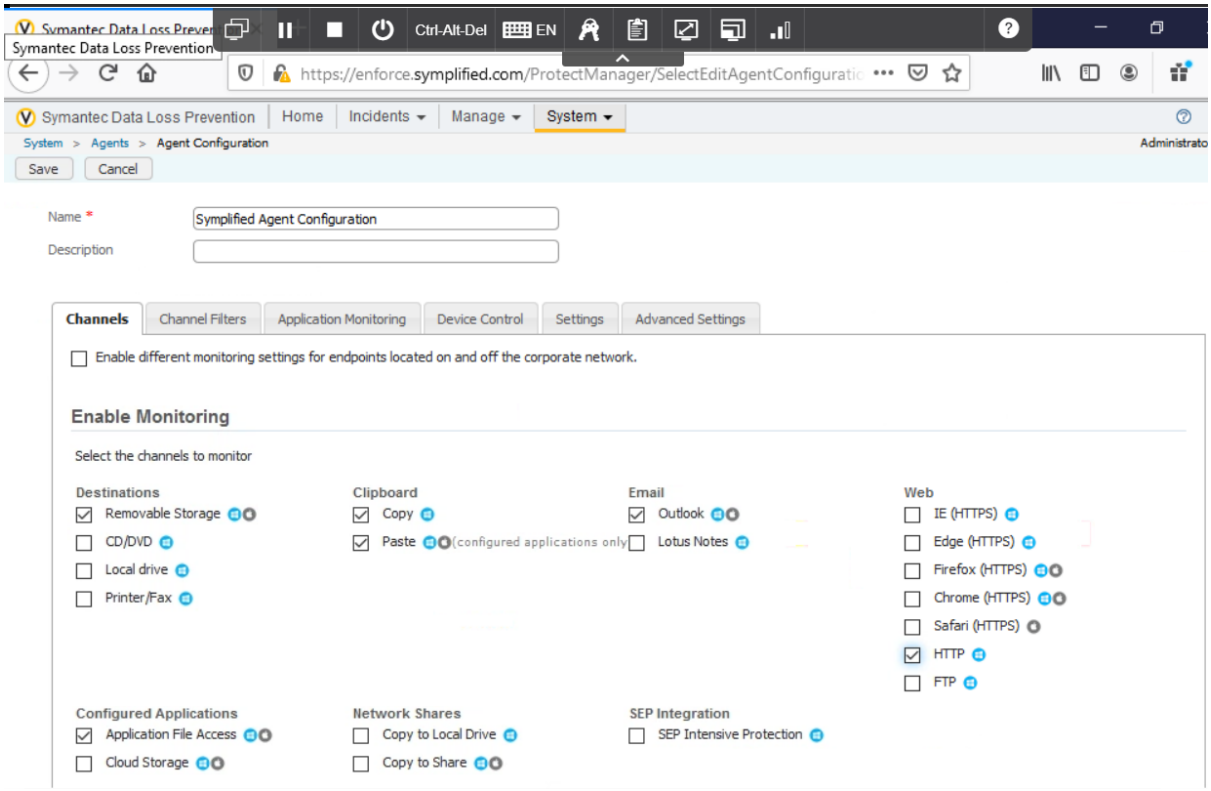


Since there is no OCR engine

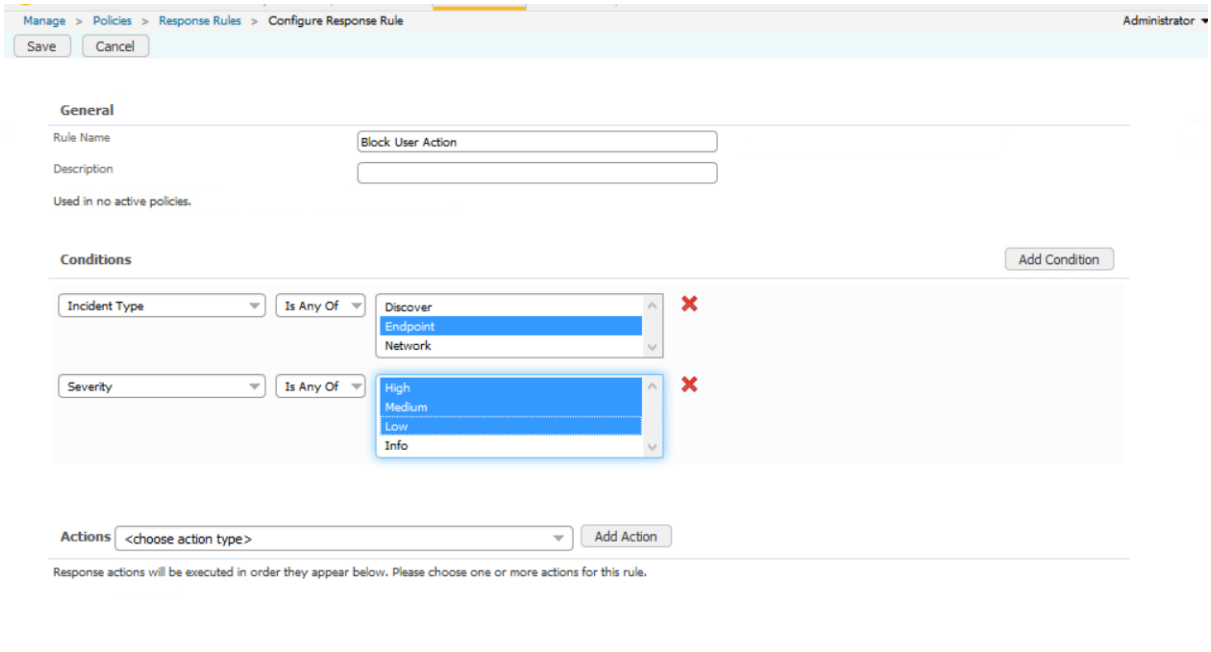
Exercise 3:

Configure Endpoint blocking.

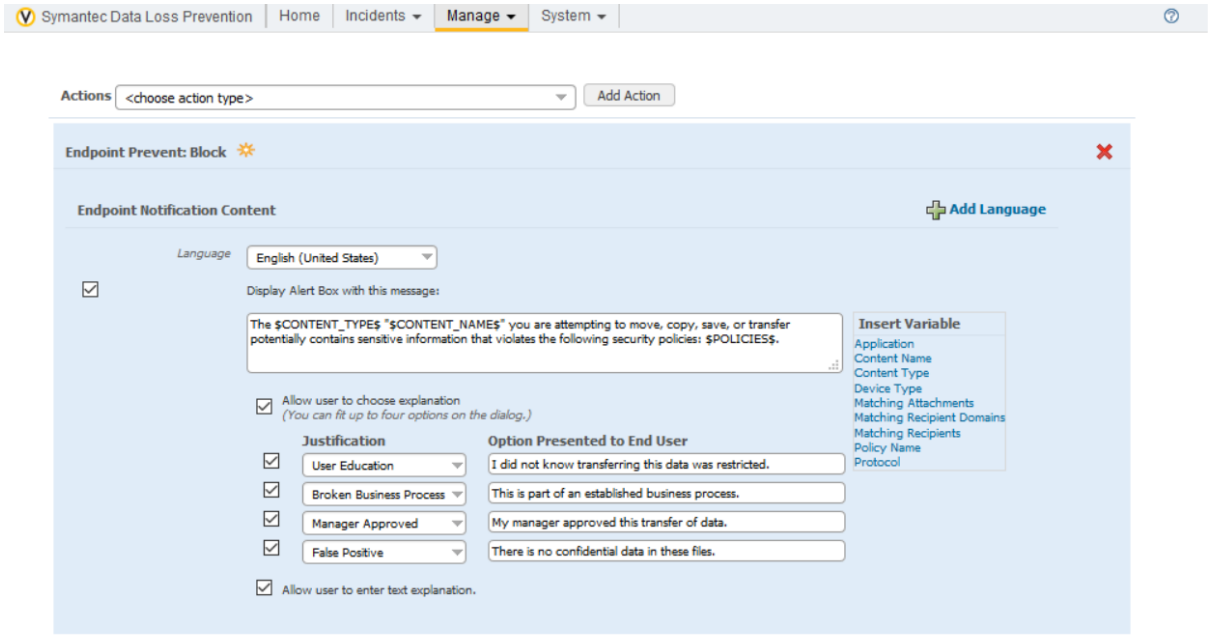
Blocking the sensitive data at the end is the best option if an endpoint user is unable to handle the sensitive data properly we need to block the data at the endpoint.



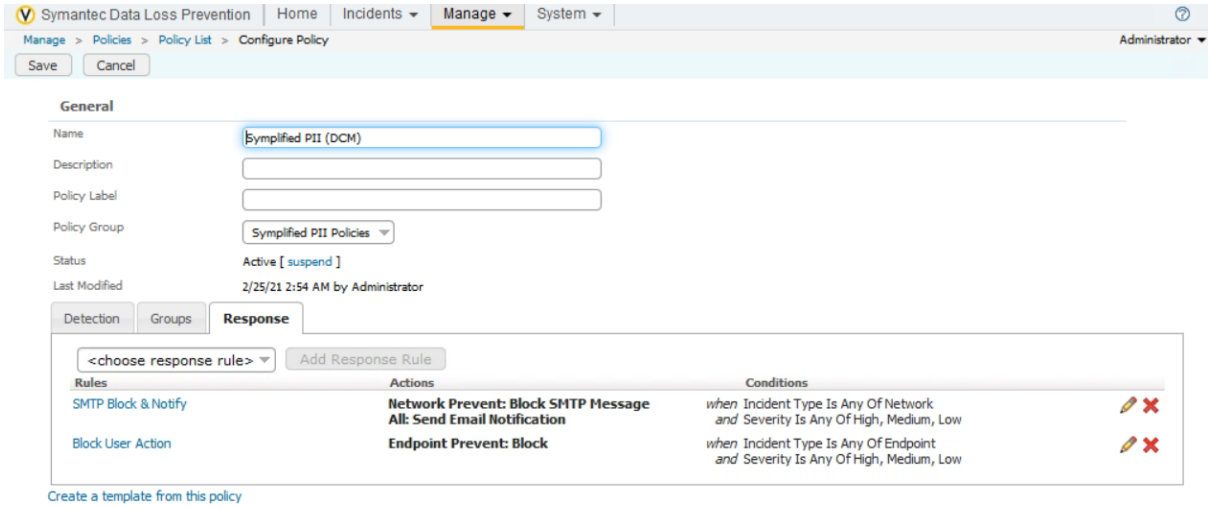
Http is checked in the web.



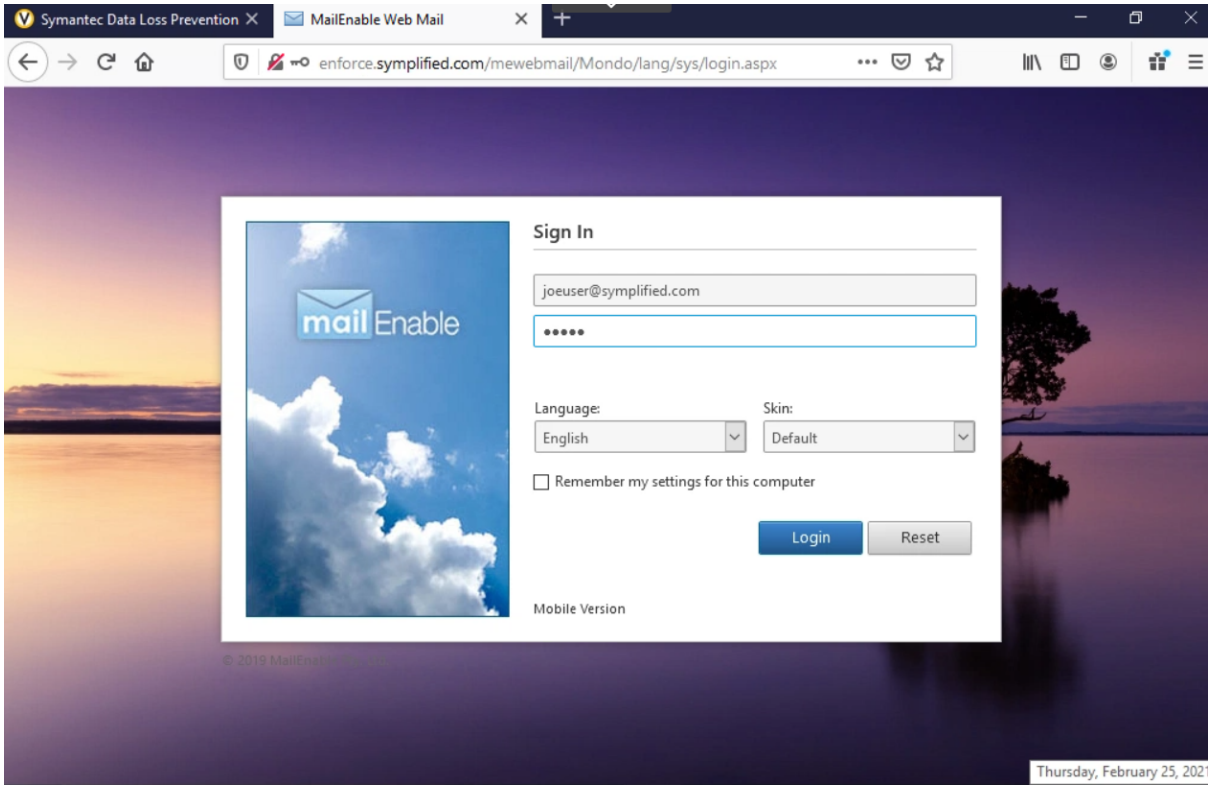
Configuring the response rules



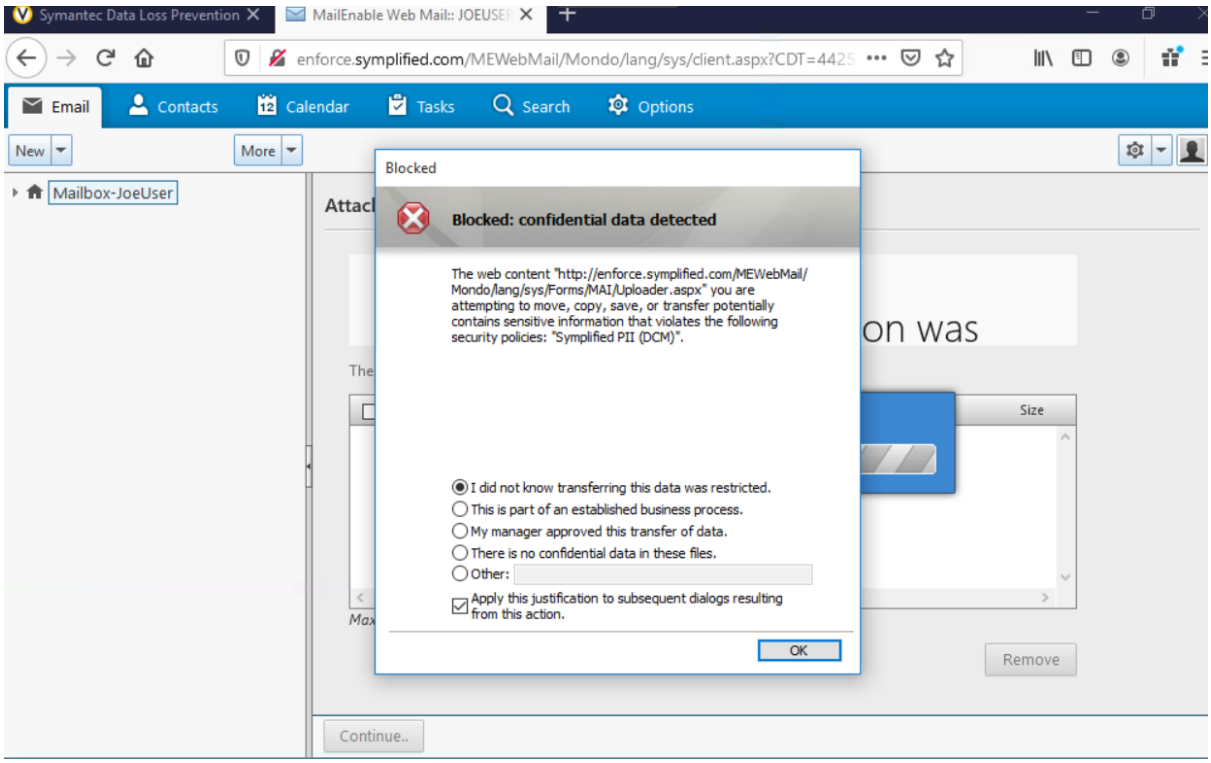
Configuring the action upon the policy violation



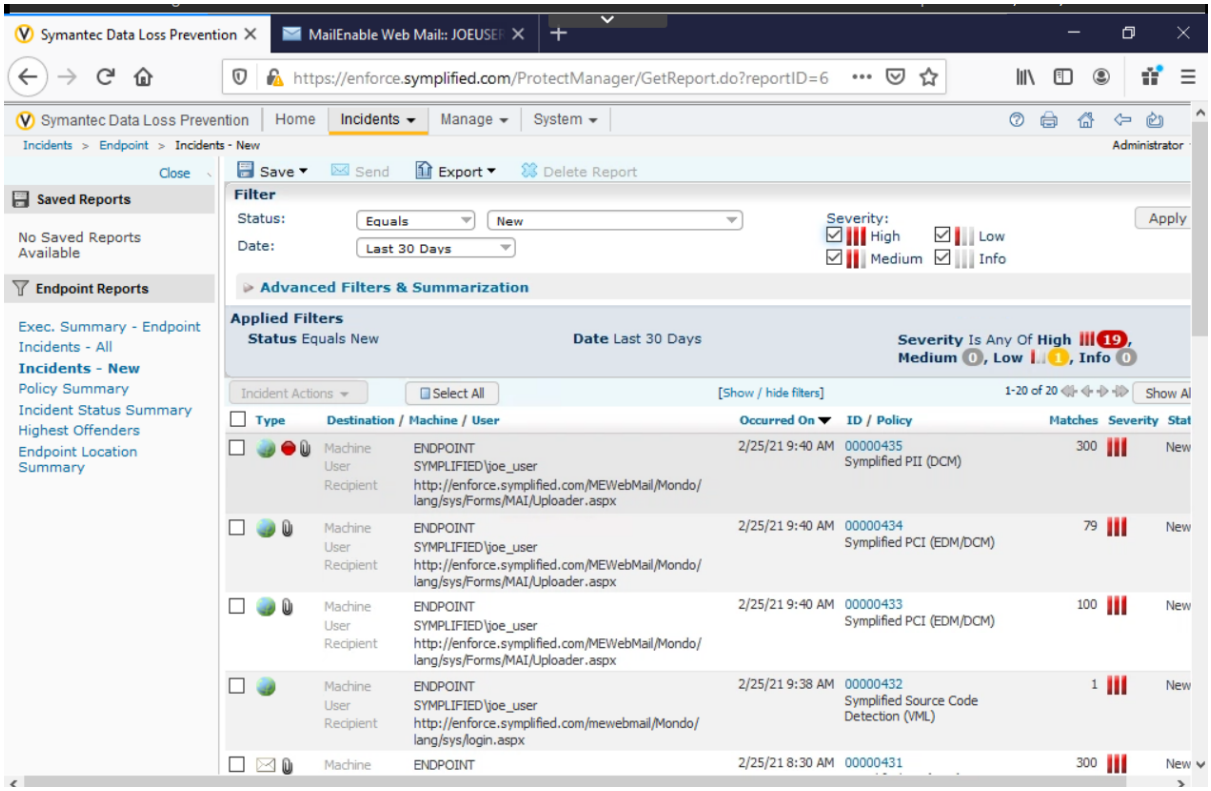
Blocking the user action by changing it in the response tab.



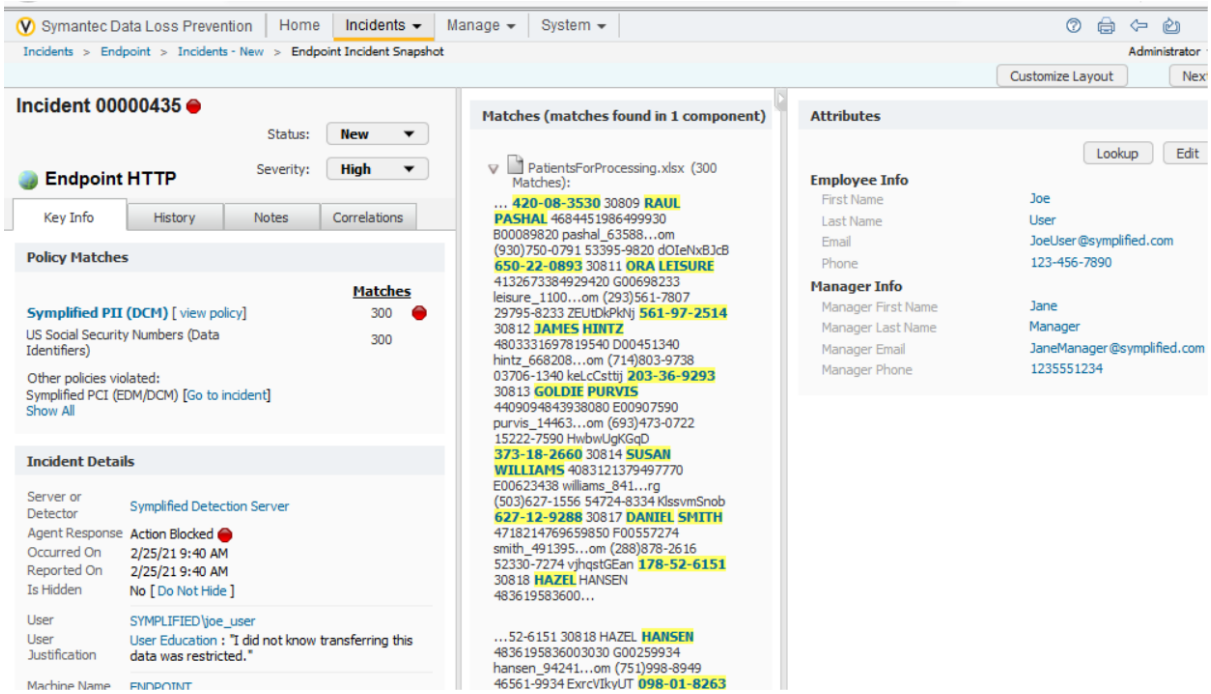
Accessing the web mail.



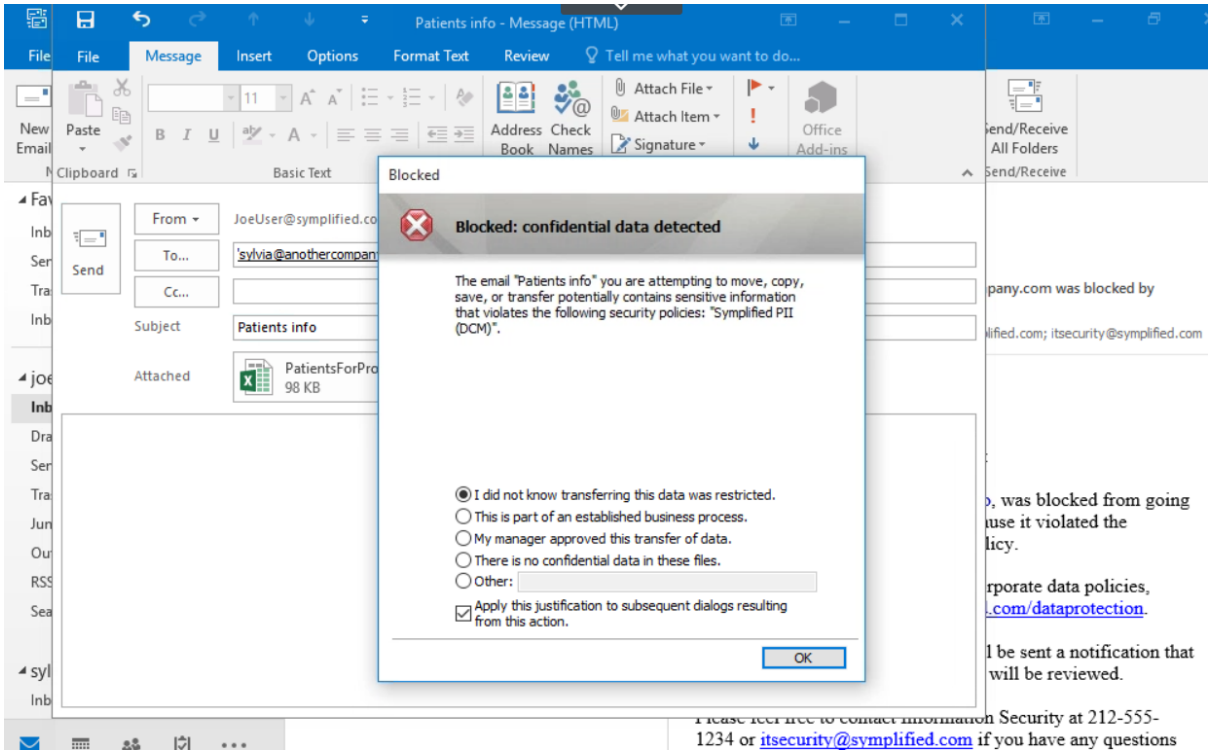
We can clearly see that it is blocking the sensitive data from sending.



Incident raised at the endpoint.



In detail info about the incident red dot indicates that mail was not sent.



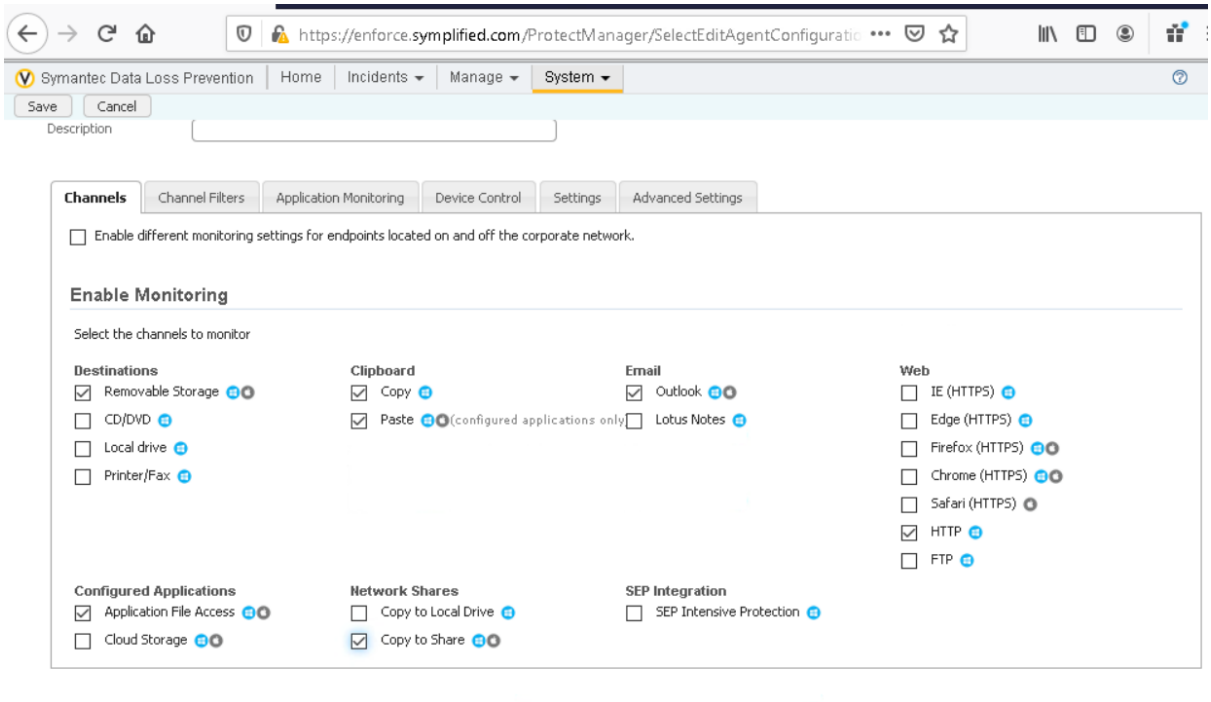
I tried sending the mail from outlook app as well the same error has occurred and its blocking the sensitive data from sending to the recipient.

Vinay Kumar Reddy Donda dondavinayreddy@gmail.com

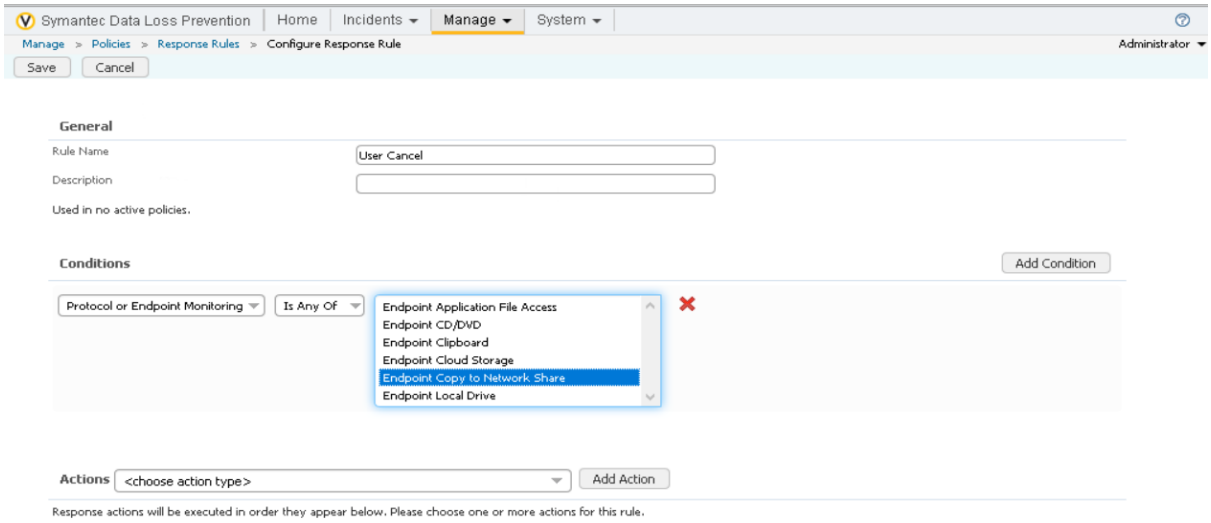
Exercise 4:

Configure end point user cancel

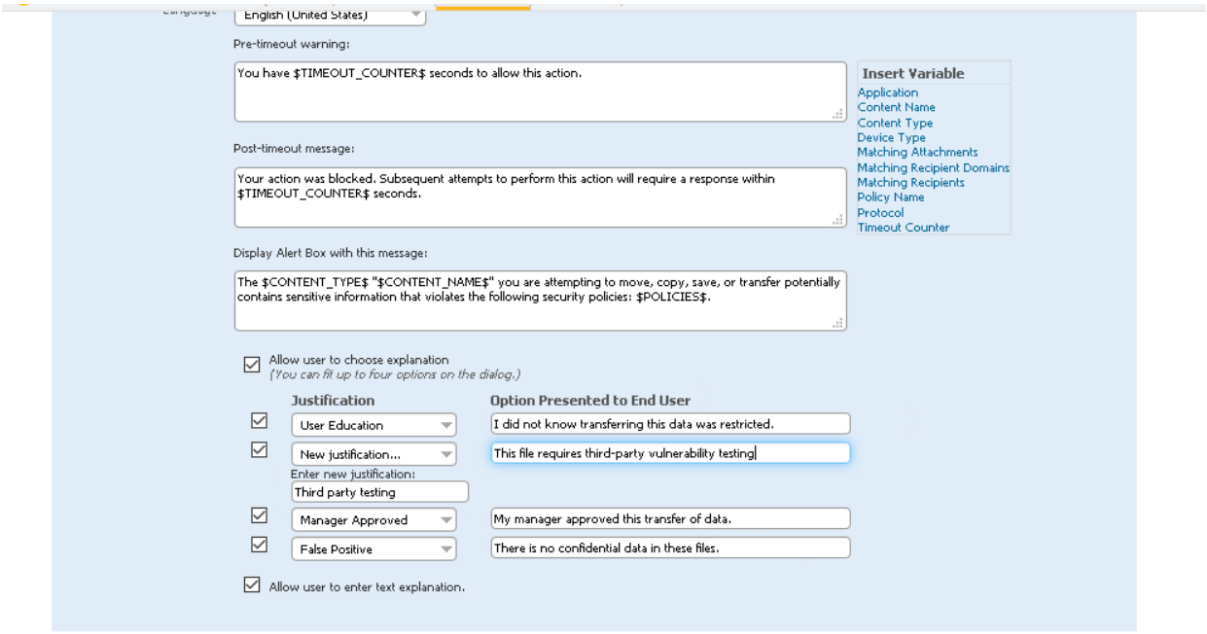
Symplified employess working on new project and they are supposed to check in all code to the git repository. Actually the rules are like no source code should be stored on network drive but there are some instances when a file needs to be stored on a network share for vulnerability testing by a third party. In that case before allowing a file to be copied to the network share, simplified has chosen to block any project halo files but allow the user to consciously decide if the copying is the right action.



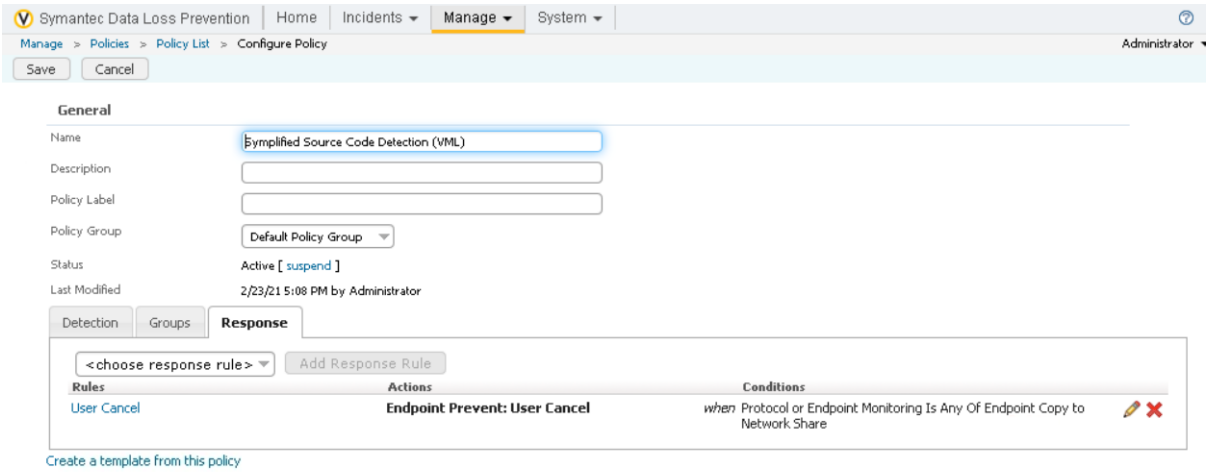
Enabled copy to share in network shares.



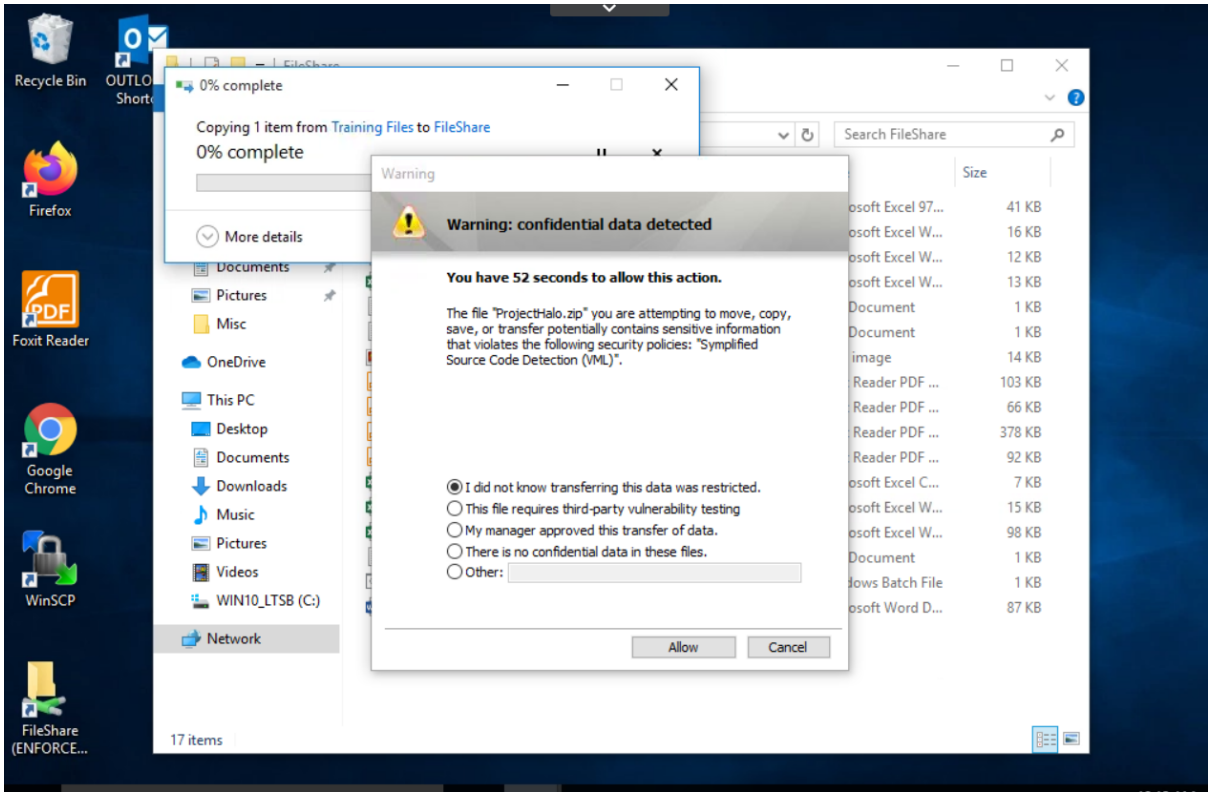
Configuring the response rules



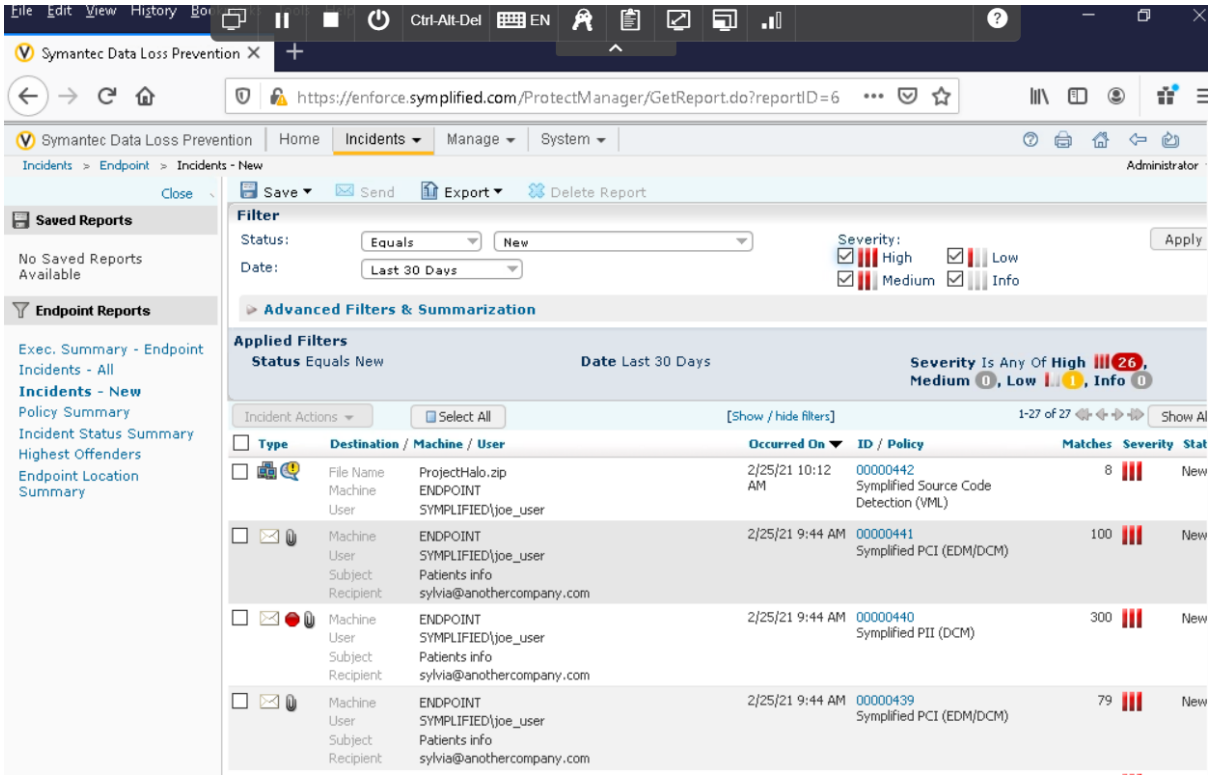
Configuring the rules



Configuring the policy

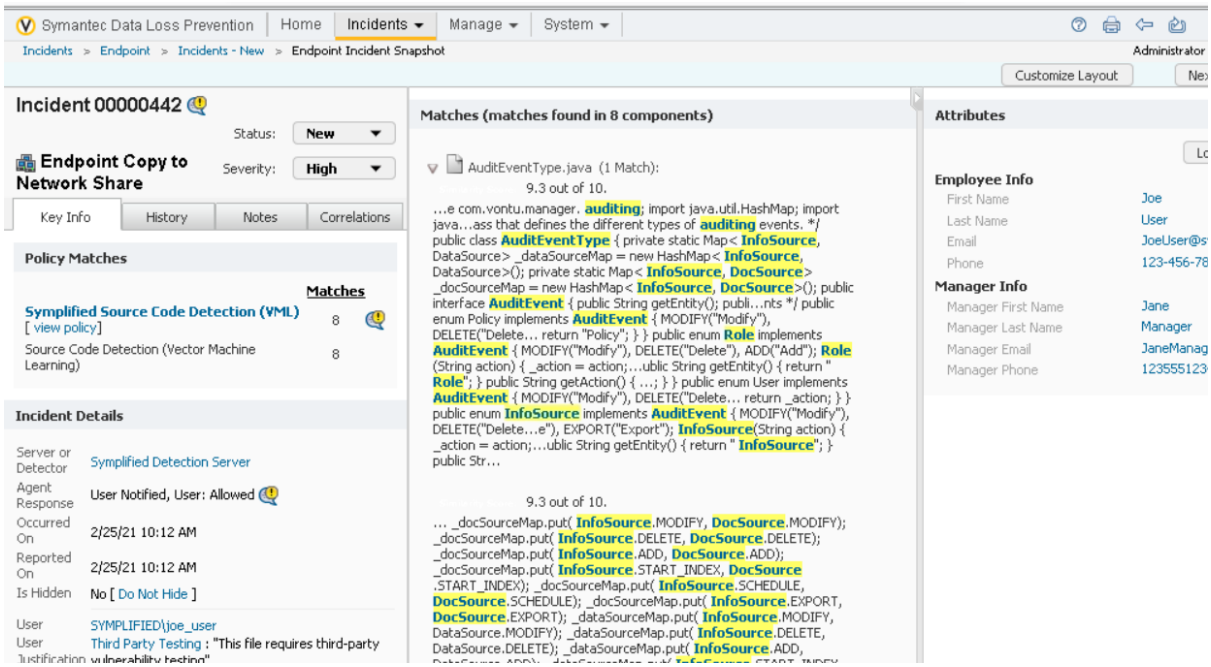


A warning is getting while copying the data and after selecting the appropriate reason it will copy



Incident is risen at the endpoint

Vinay Kumar Reddy Donda dondavinayreddy@gmail.com



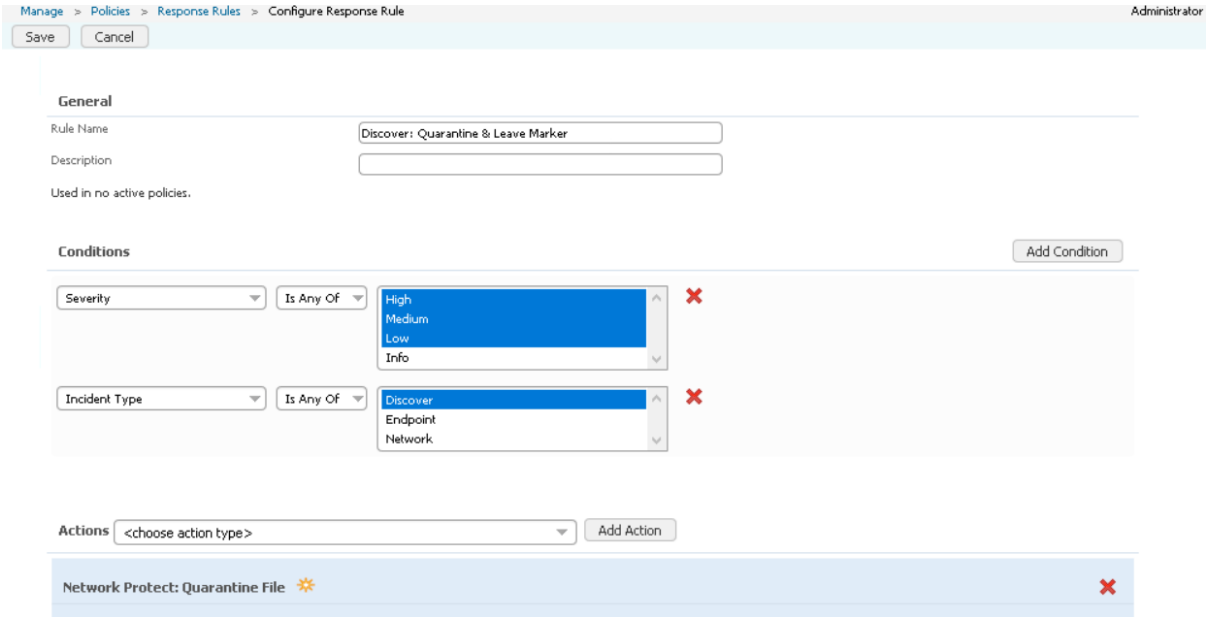
Detailed view of the incident.

Exercise 5:

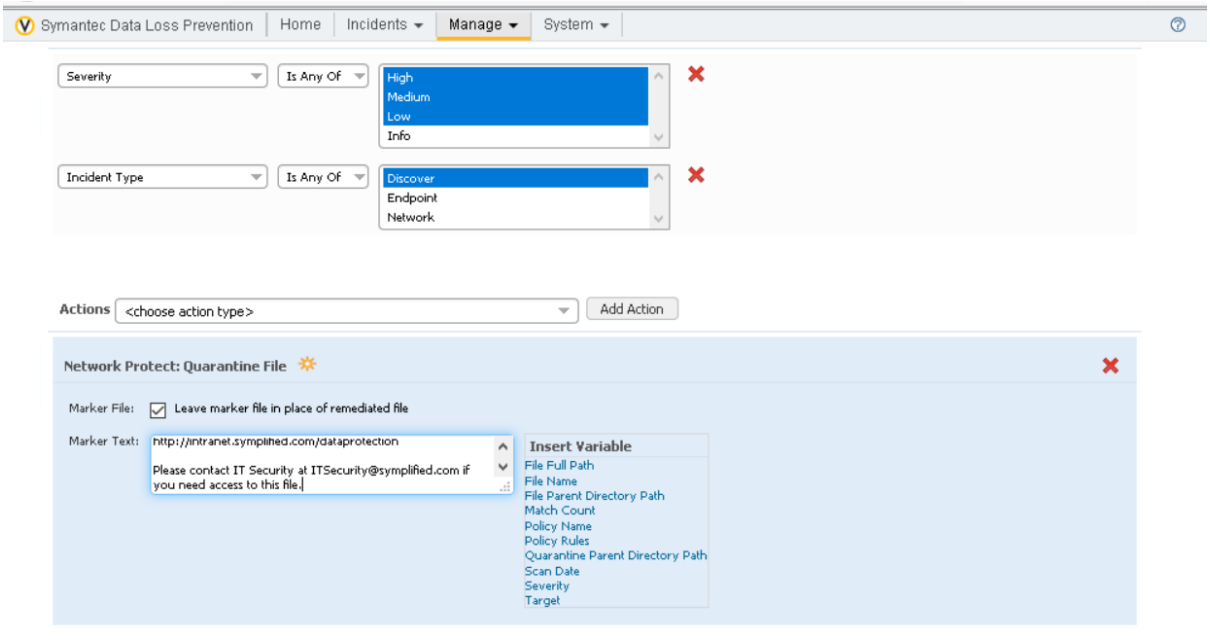
Scan and quarantine files on a server file share target.

Earlier, Symplified scanned and found all open shares and configured a windows file share scan to scan the shares. They have now decided it is time to begin quarantining the files found in these shares to a secure file share on the network.

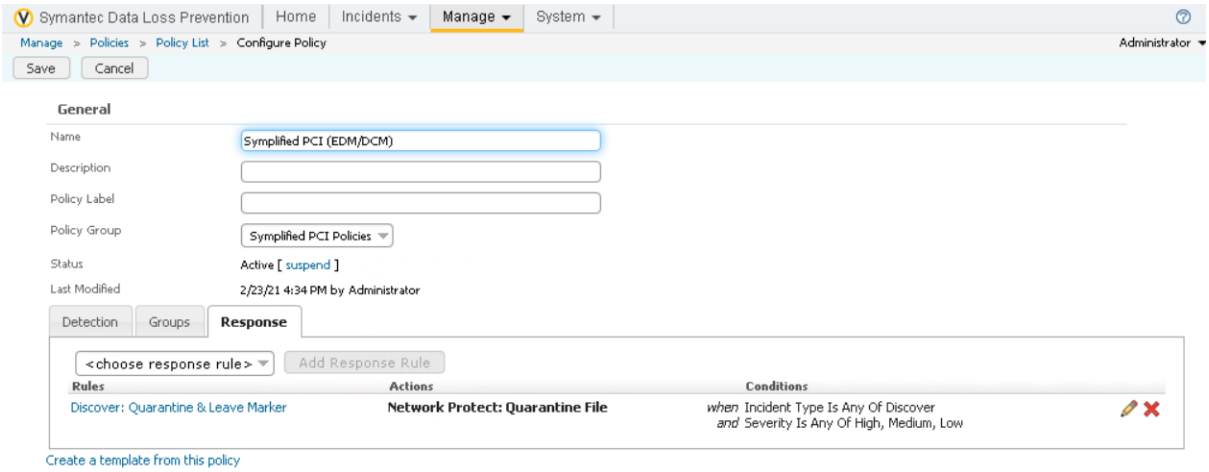
In addition to quarantining the files, a marker file will be left in the place of the orginal file. This marker file will indicate where the user can find the orginall file and how to access to it.



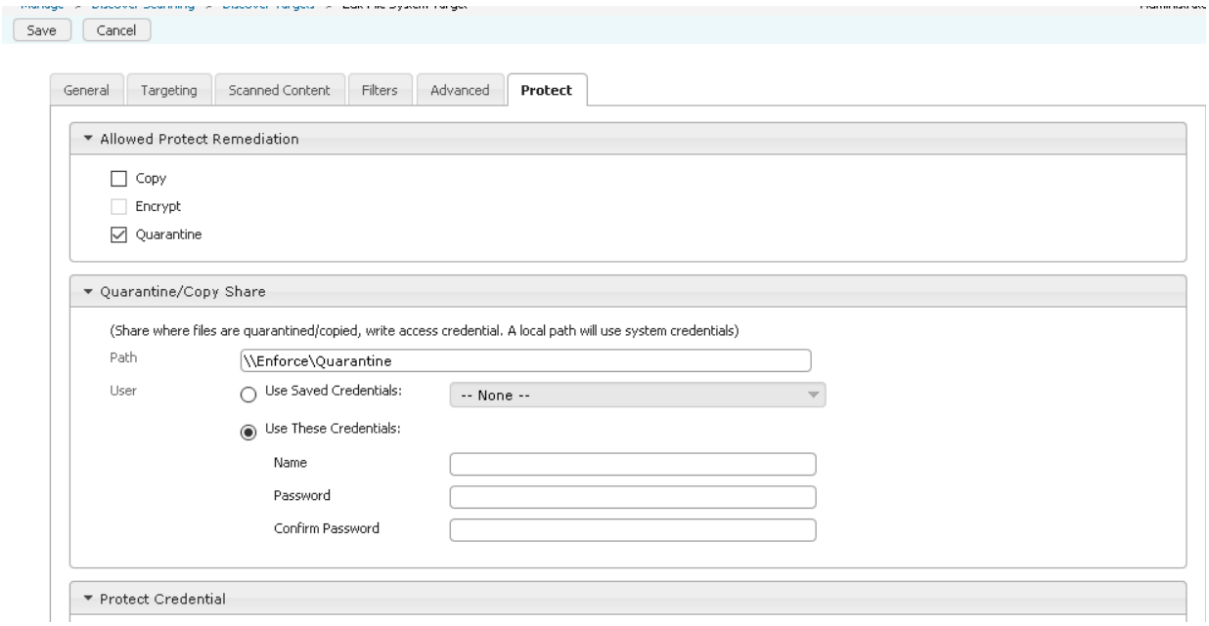
Configuring the response rules



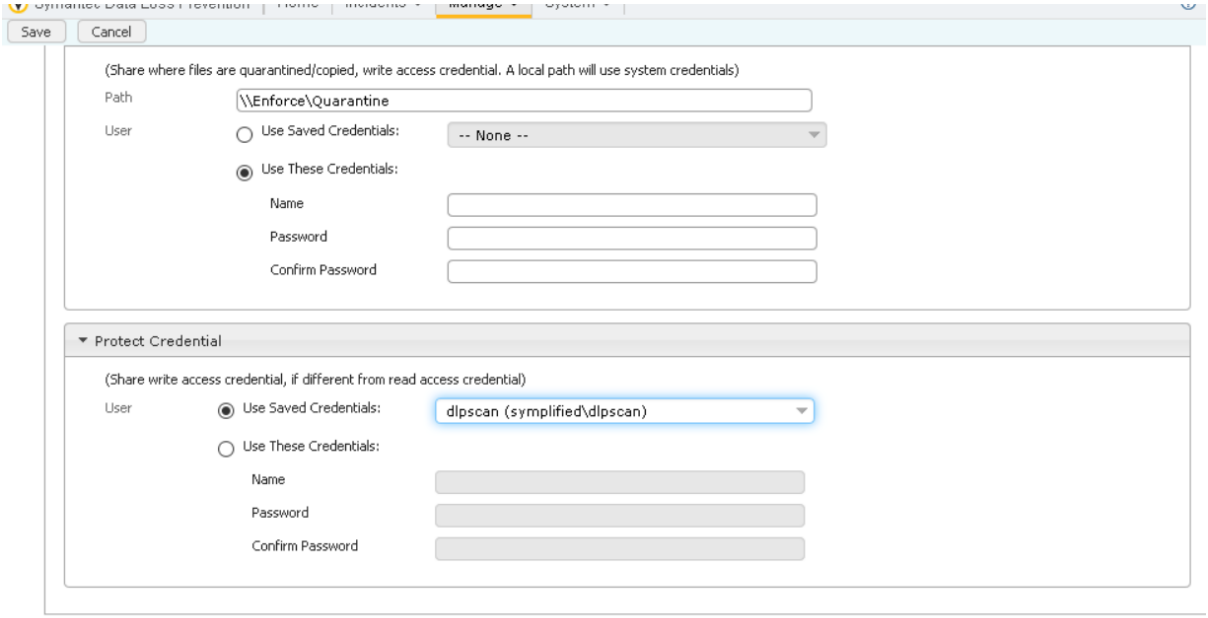
Configuring the response rules



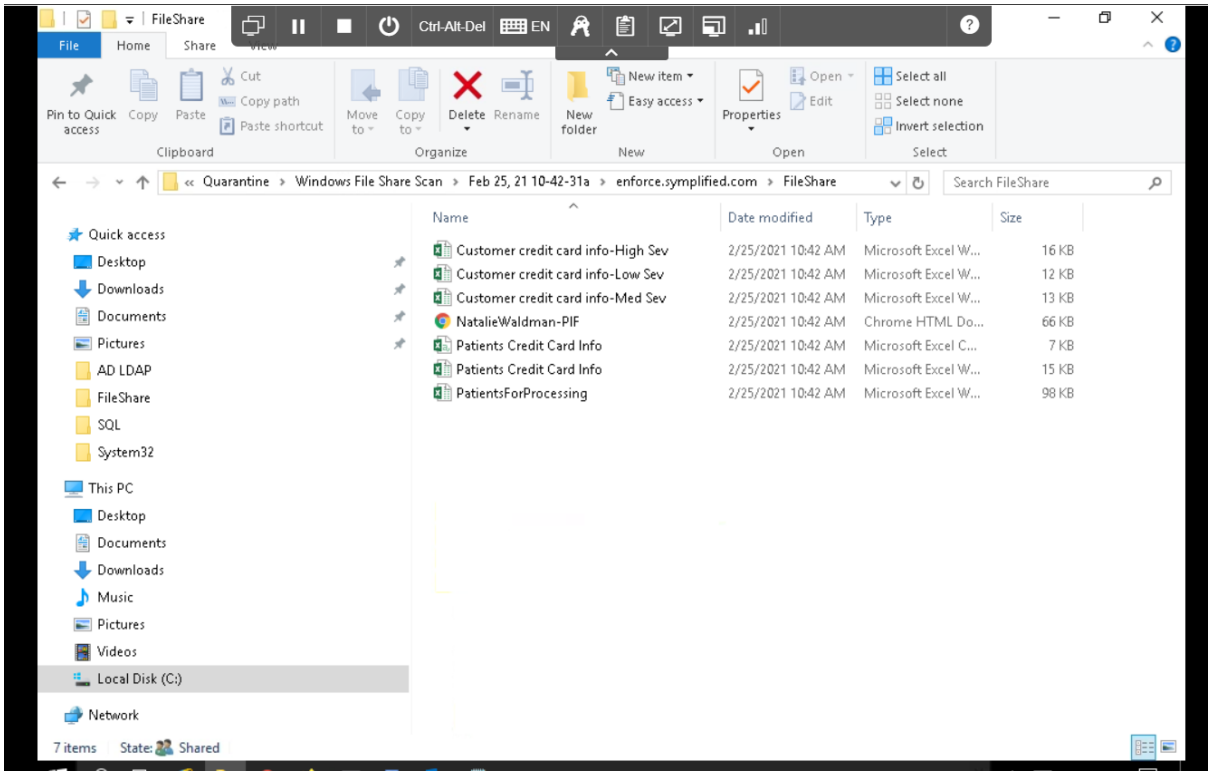
Configuring the policy and response to it.



Editing the protect (File system Target)



Editing the file system target.

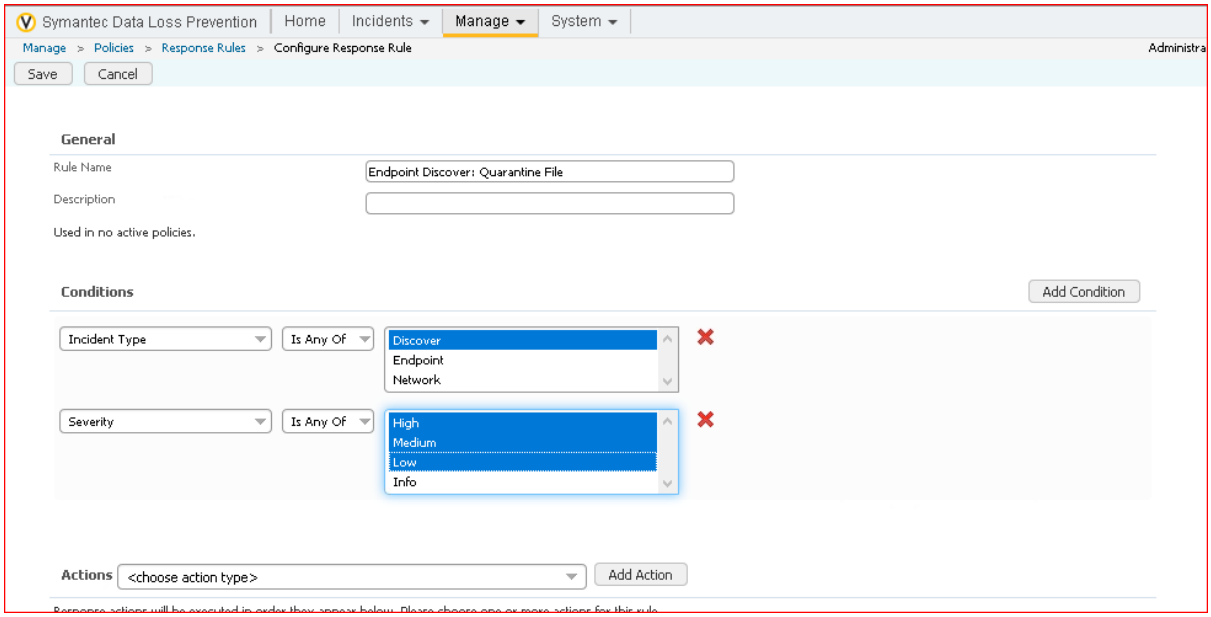


Analayzing the file of the located incident.

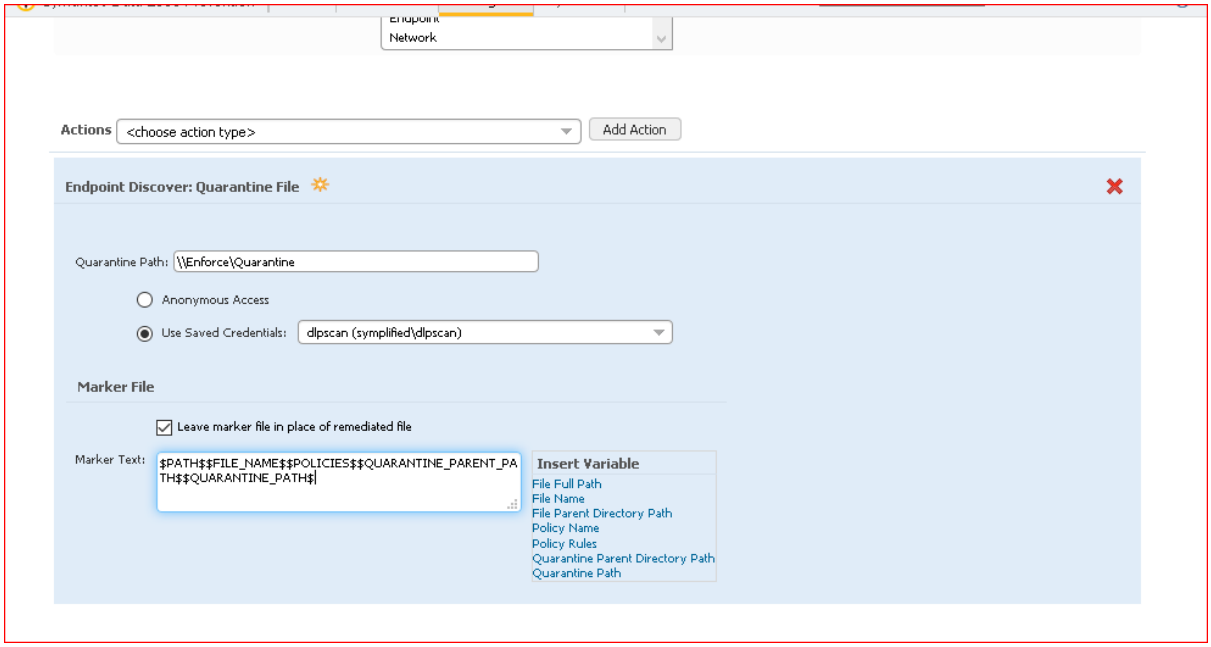
Exercise 6:

Scan and Quarantine files on a endpoint target.

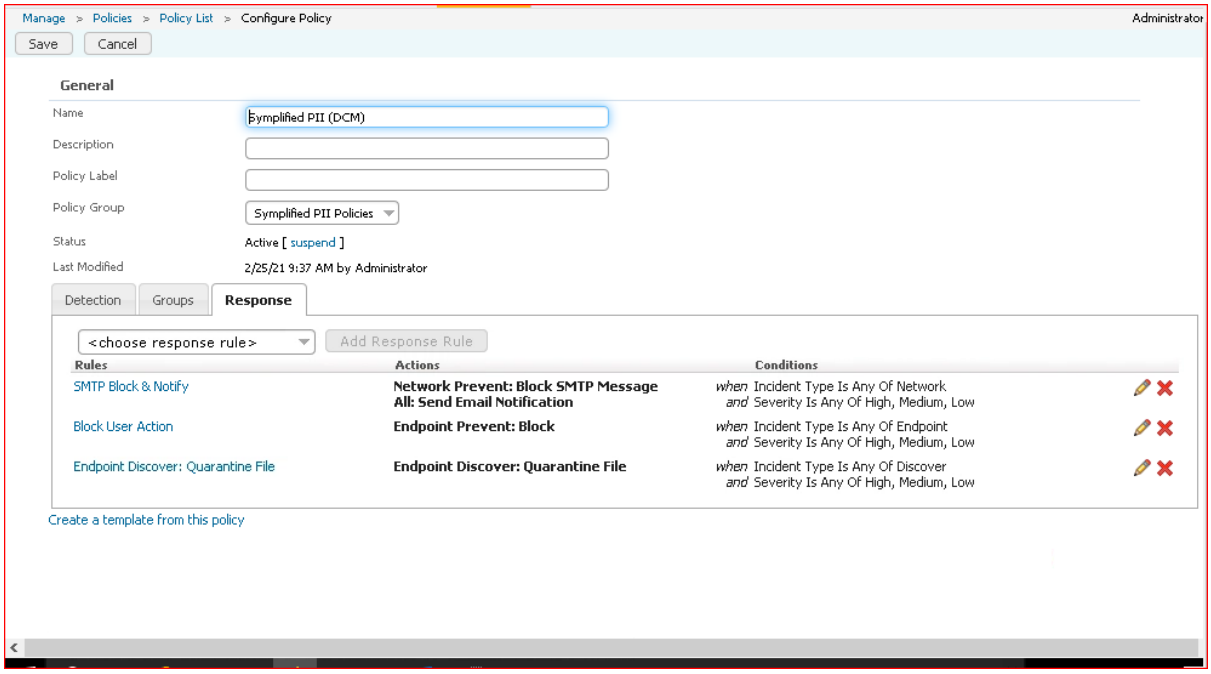
Till now, we scanned and quarantined the files which are transferring the network but in this lab we are going to scan and quantraine the files even before travelling through the network i.e., at the end point.



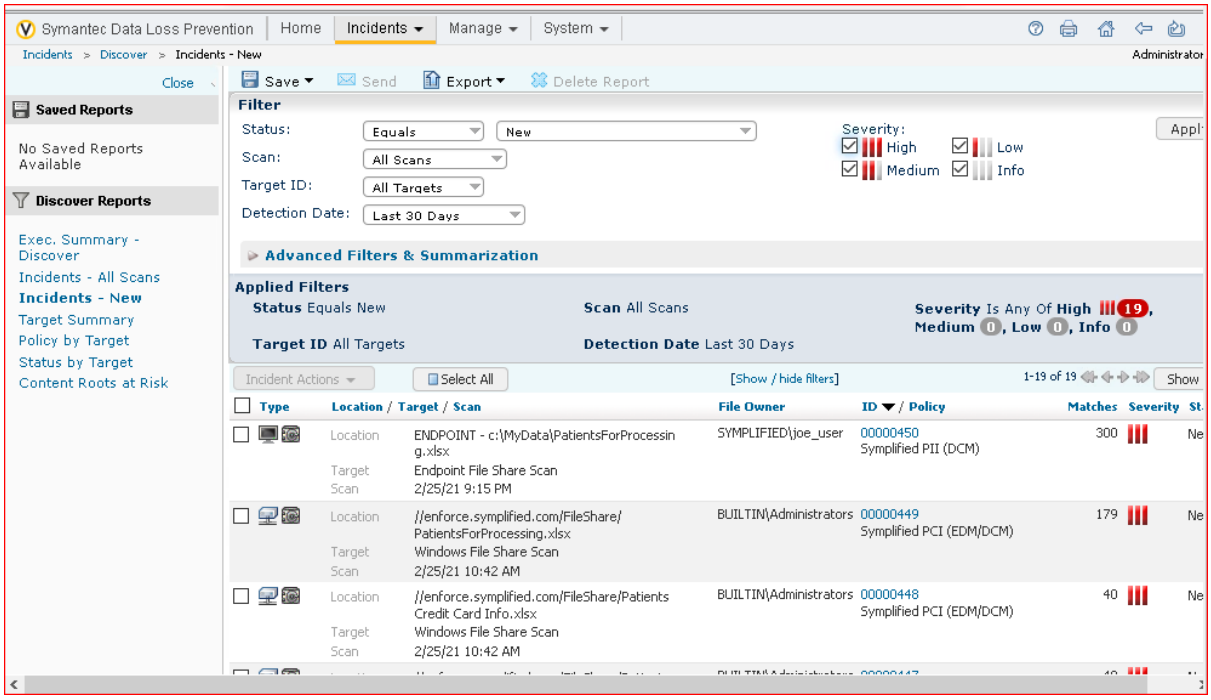
Configuring the response rules.



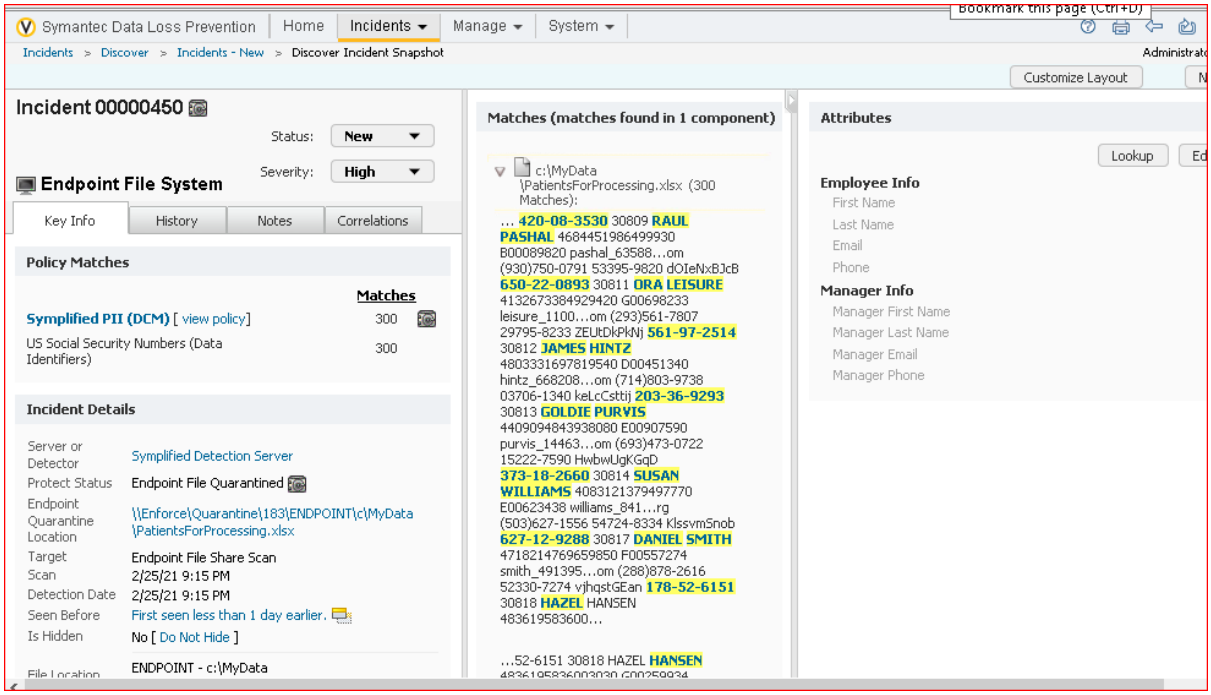
Composing the new custom market test using the insert variables



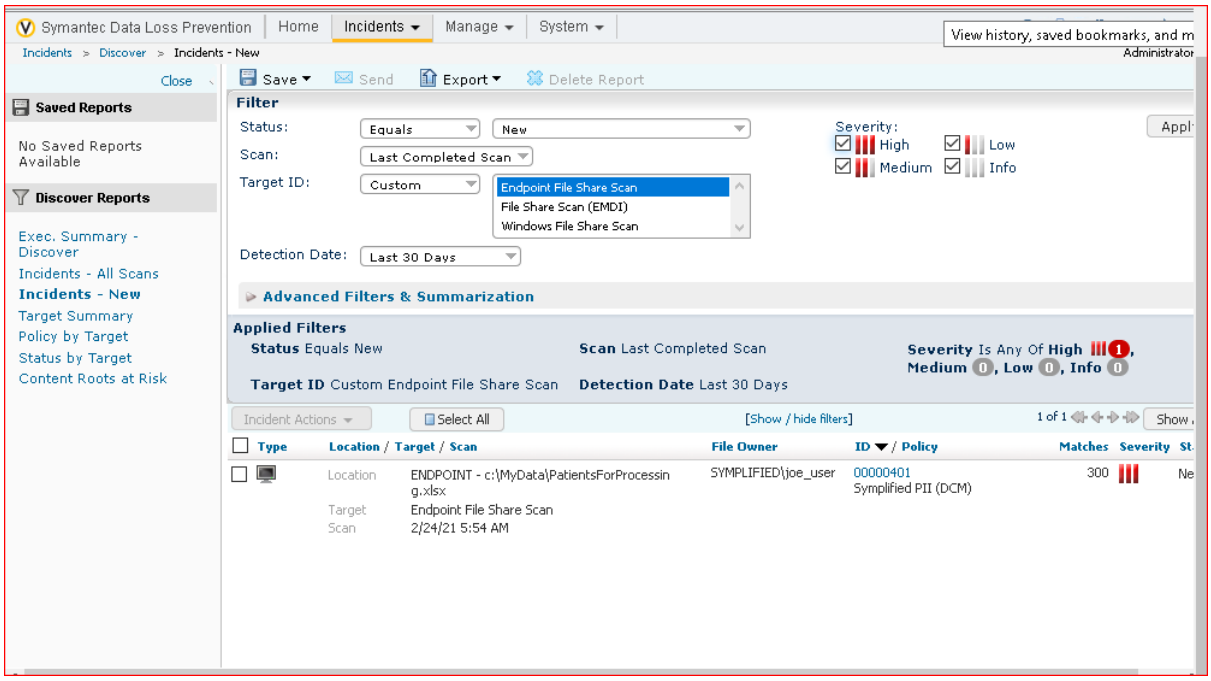
Adding the response rules.



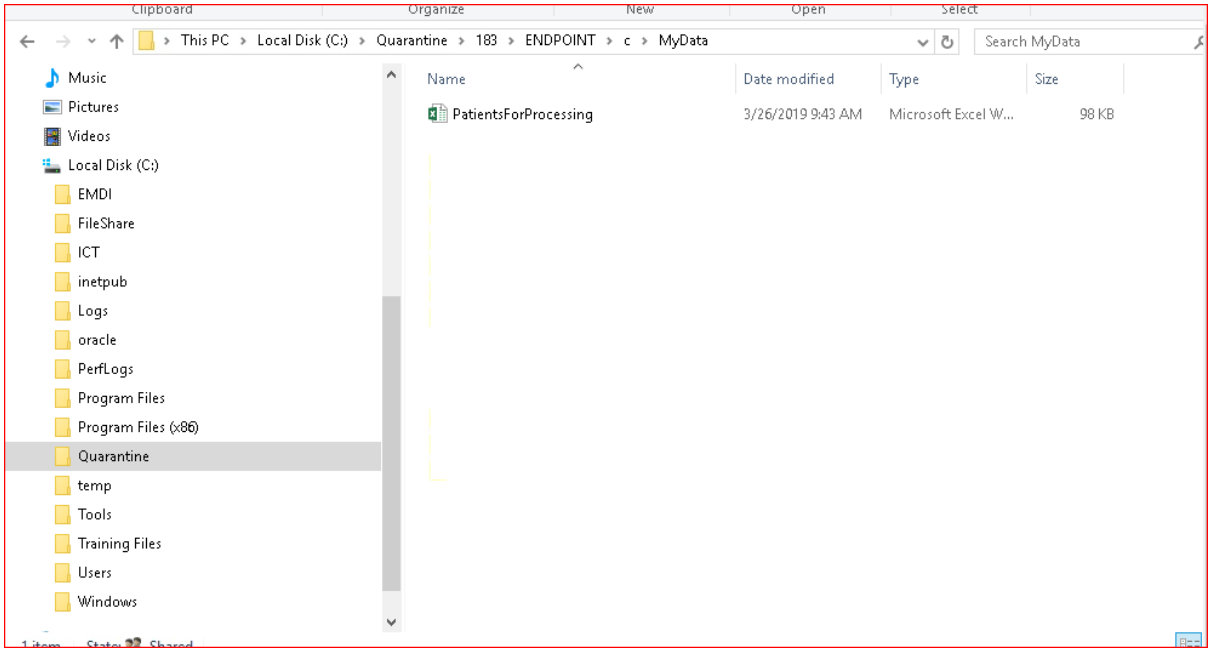
We can clearly see that incident is generated



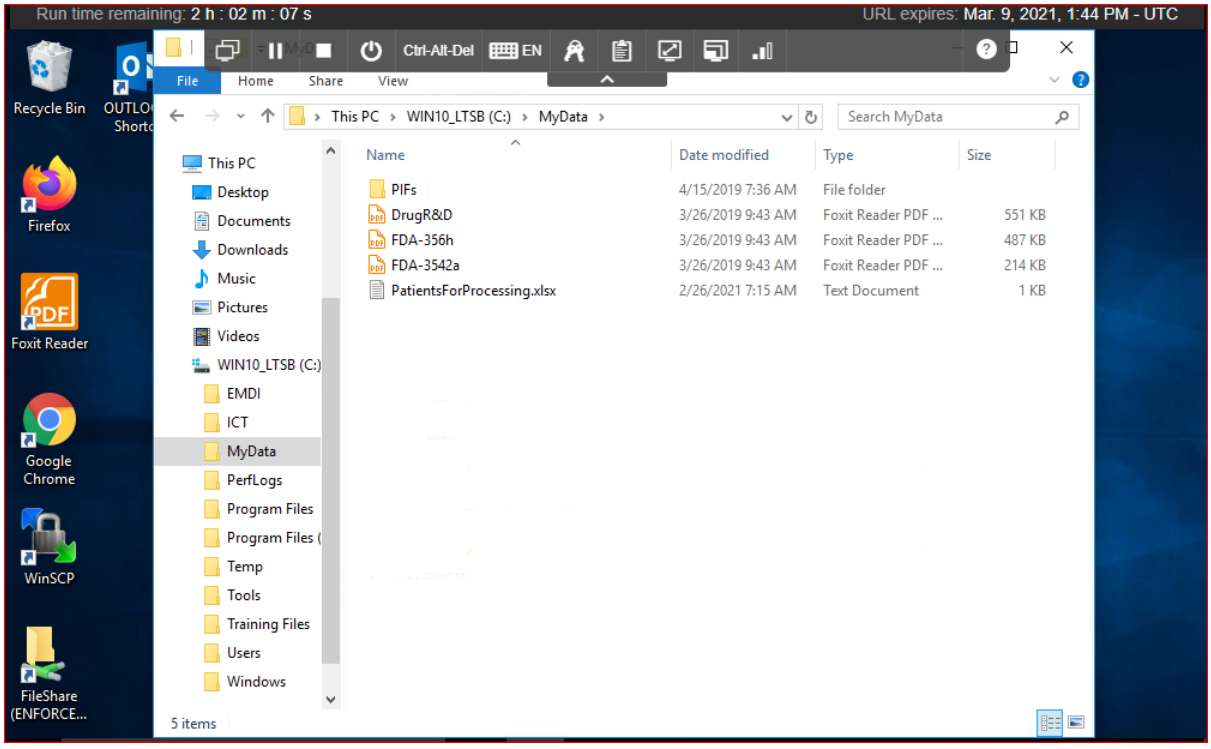
In detail view of the incidents.



Incident at the endpoint



File is Quarantined.



Even at the endpoint in my data the endpoint as well.

Lab 6:

Remediating the data loss incidents and tracking risk reduction:

This is very important phase because once after implementing the policy voliations the steps we have done till now I mean the exercises till now. When an policy is violated how do we identify whether a user is done with carelessness or intentionally i.e., malicious user and how do we track all the incidents over a period of time.

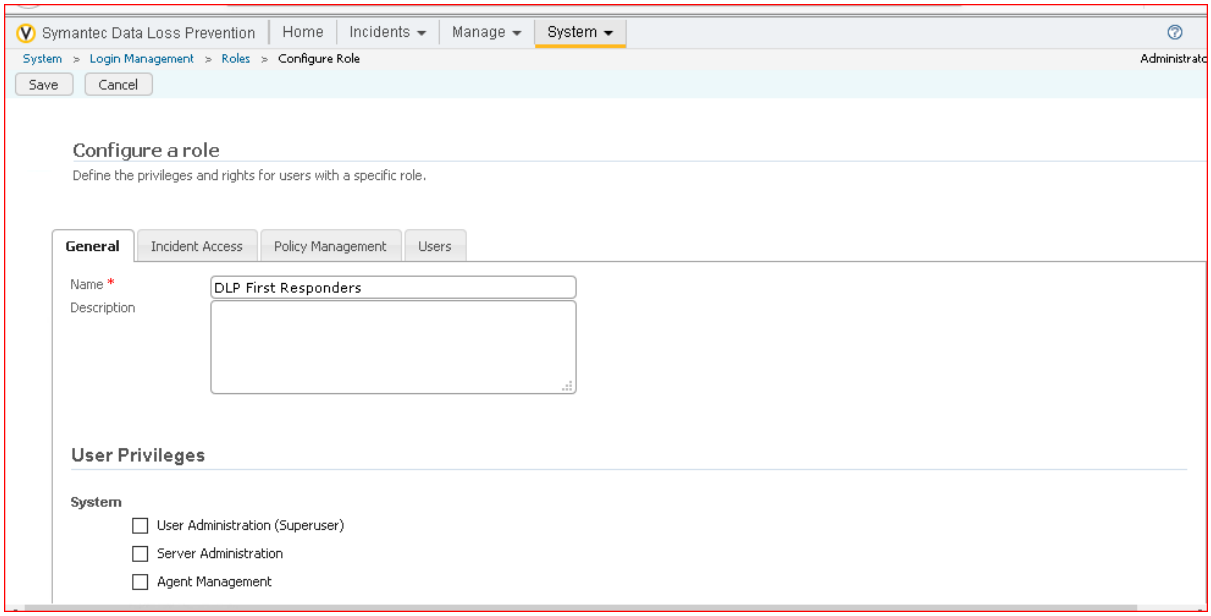
In this lab we will do about how do we assign the user roles and responsibilities and how the genuine user will view, analyze and remediate the incidents after they occurred. We will learn about the reporting capabilities of DLP's enforce server and how to generate the reports and view they by the category. Additionaly we will learn how to configure the smart responses as well which generally don't need direct human impact.

Exercise 1:

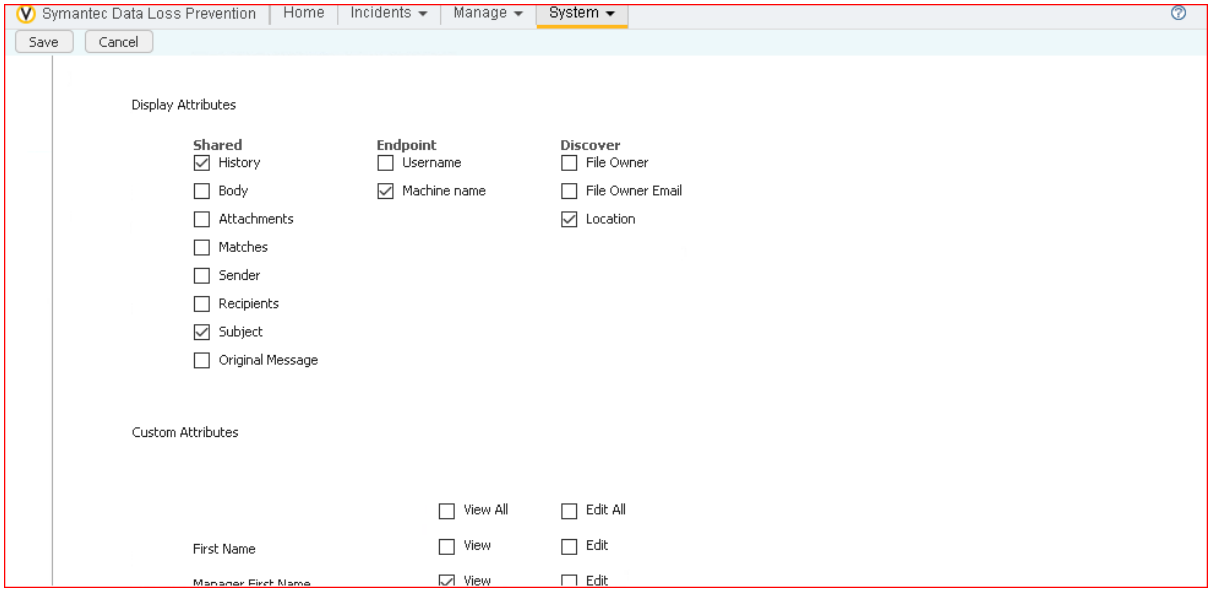
Configure roles and users.

Generally after incidents are raised we should carefully evaluate the false positives. The Symantec DLP team should have only access to view the incidents but not to make any changes in the enforce console.

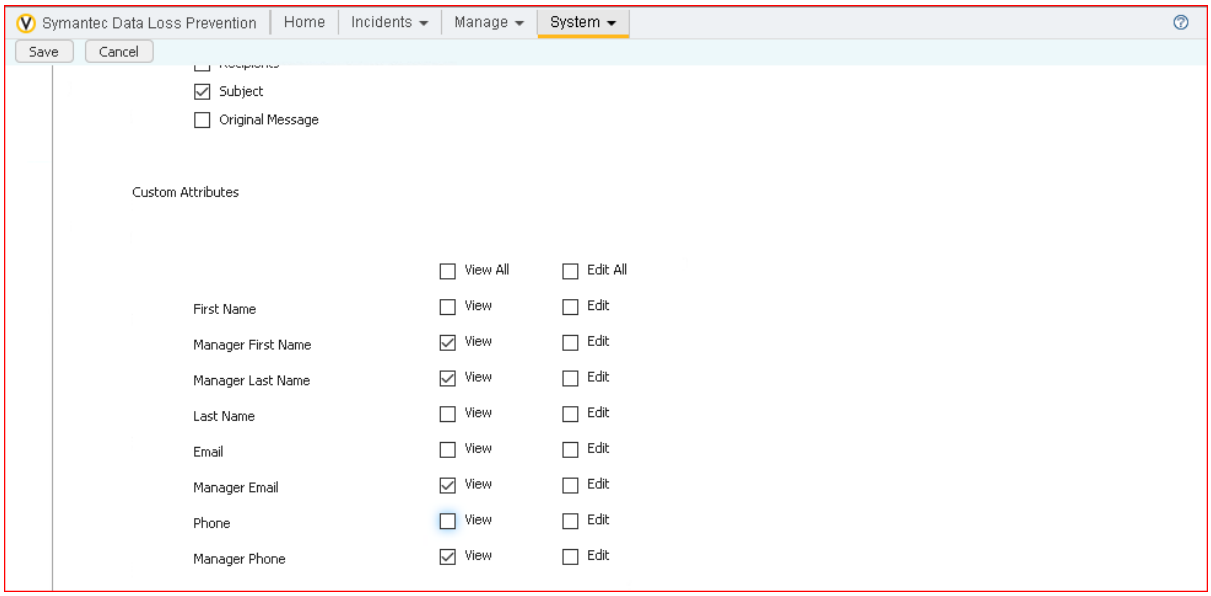
In this lab we create roles for the it team who are responsible for creating and maintain the dlp policies and response rules. A role should be created for seeing the risk reduction reports that have been created for them.



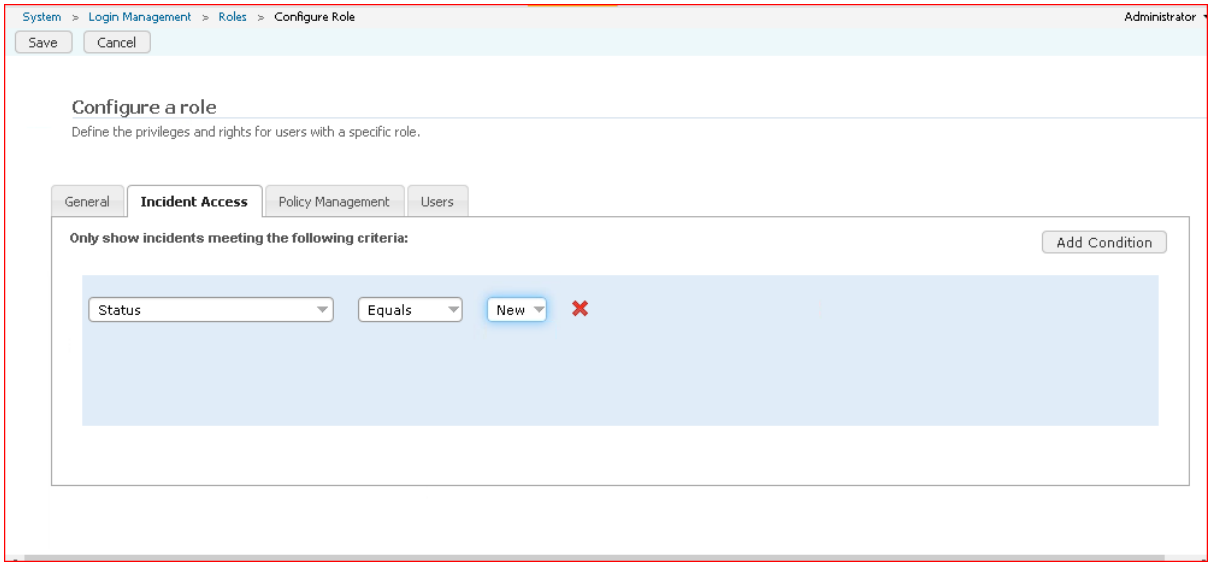
Adding the rules for DLP First Responders



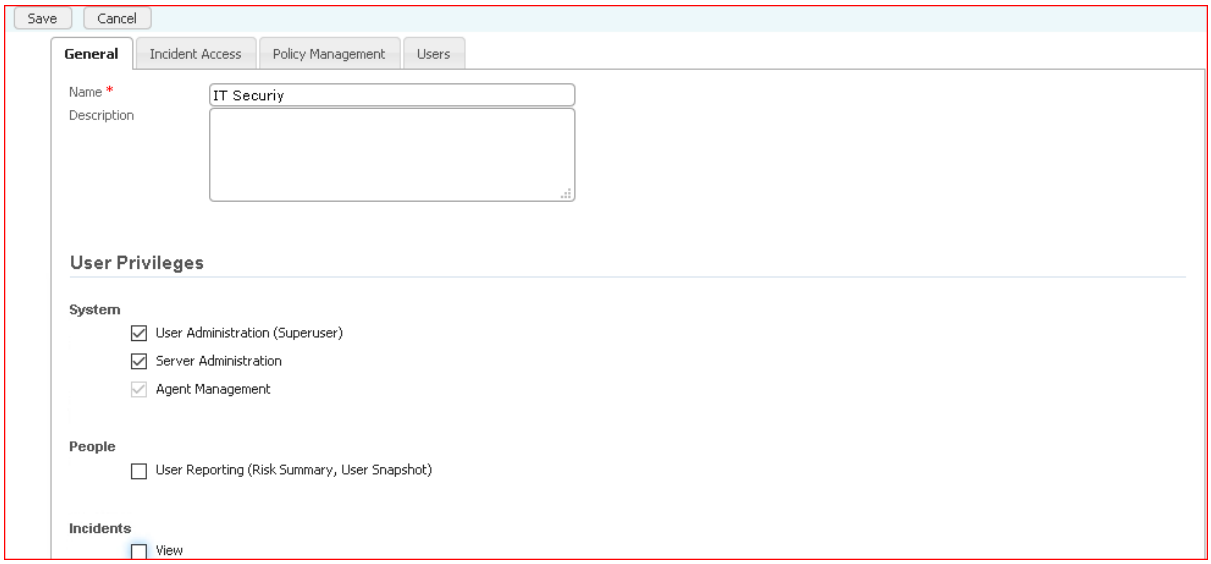
Adding the rules for DLP First Responders



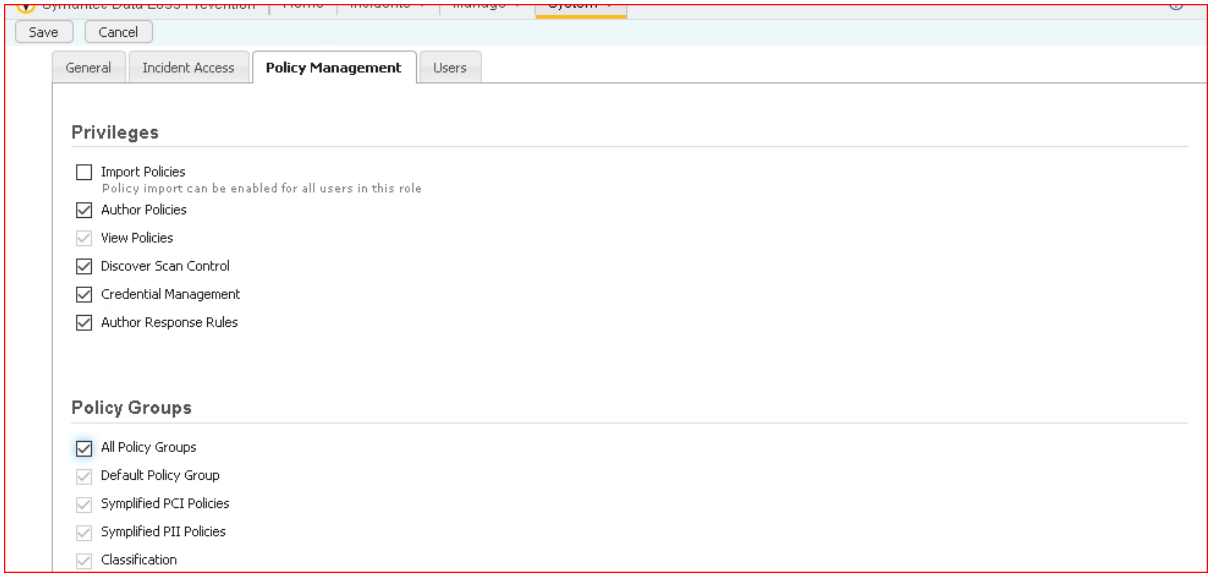
Adding the rules for DLP First Responders



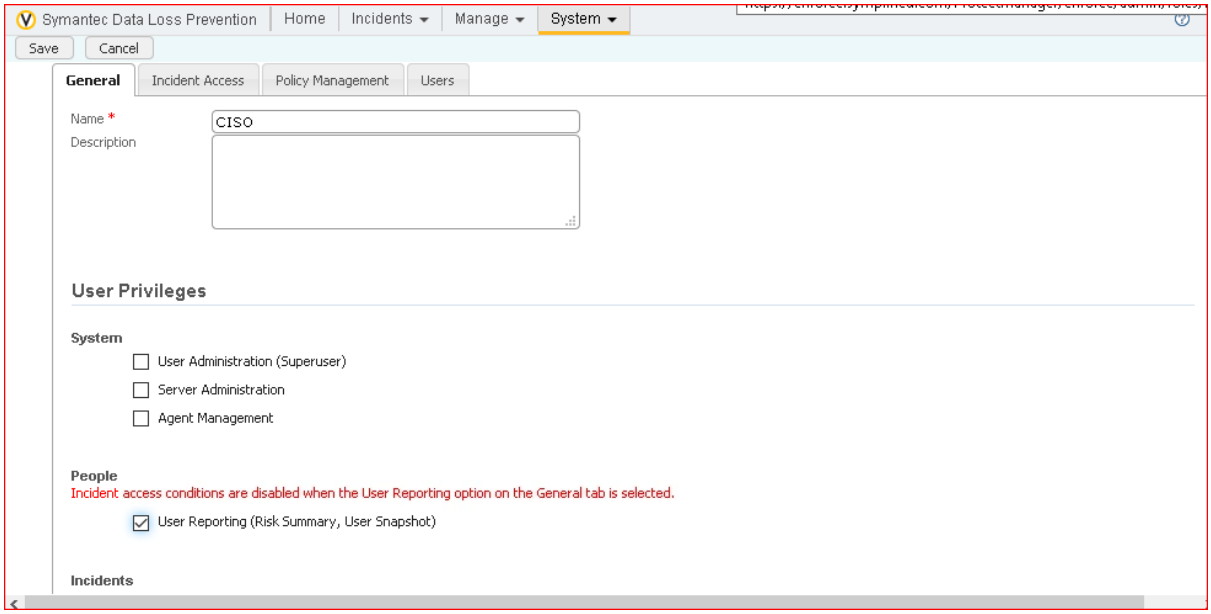
Adding the rules for DLP First Responders



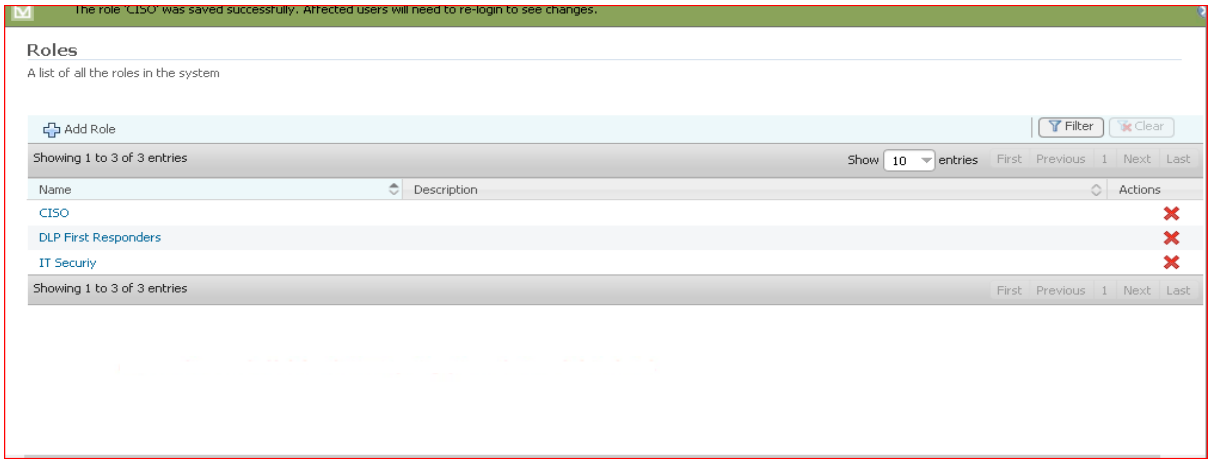
Adding the rules for IT Security team



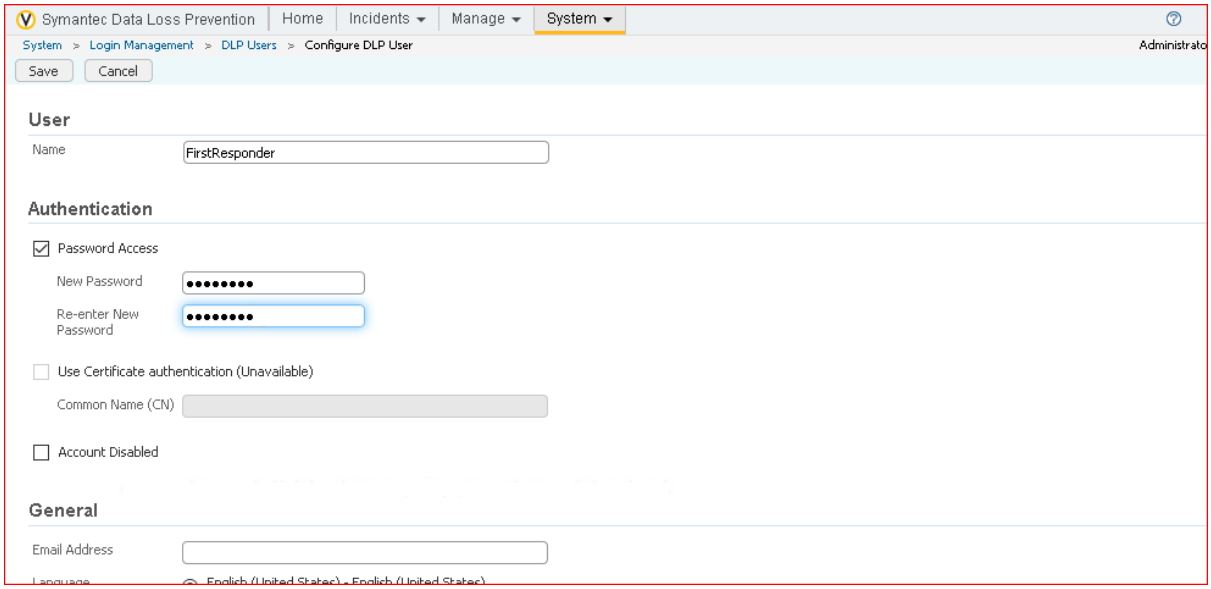
Adding the rules for IT Security team



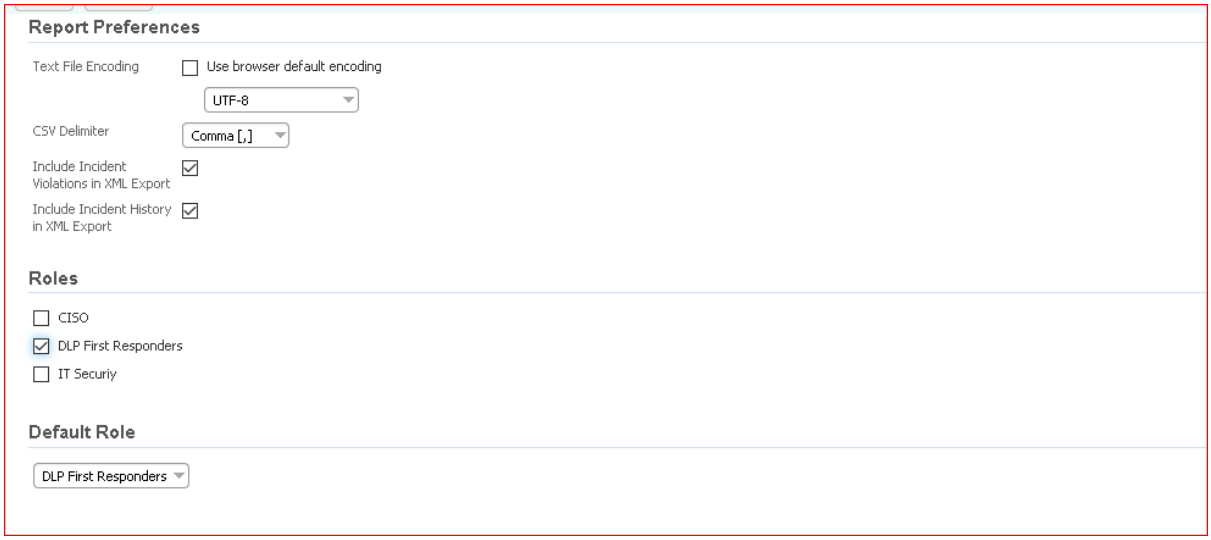
Adding the rules for CISO team



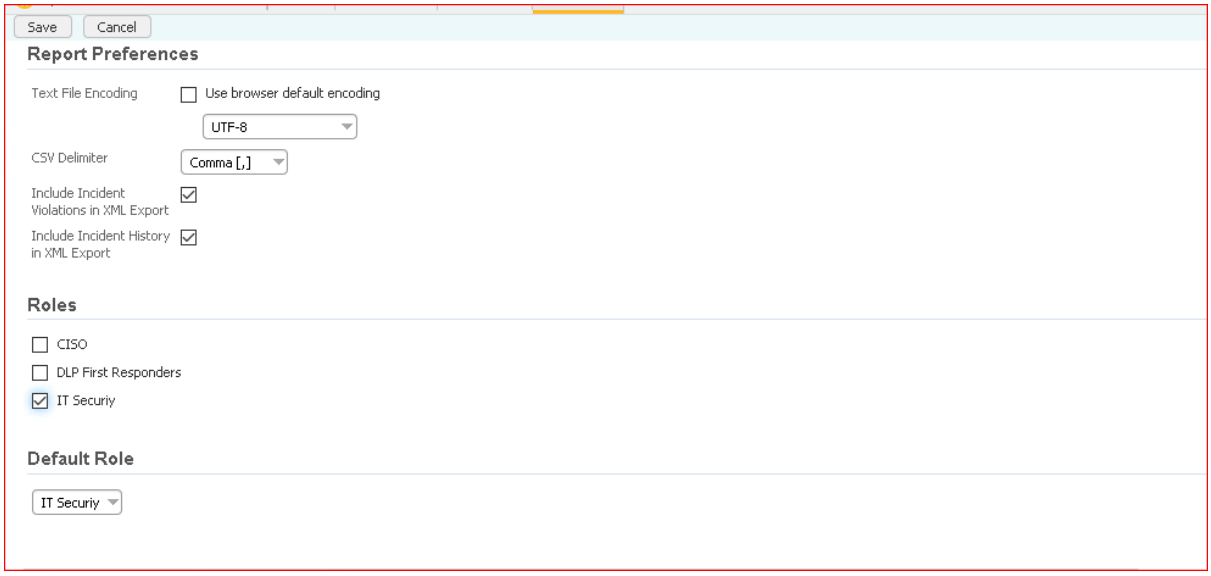
Adding the rules for CISO team



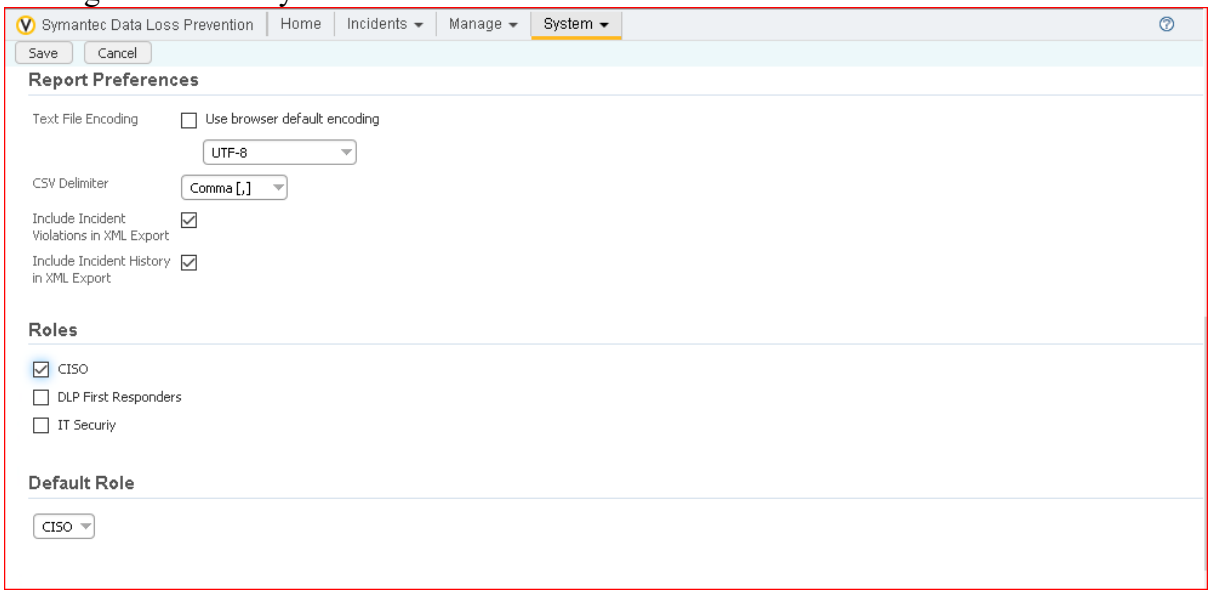
Adding the First Responder to the DLP USER



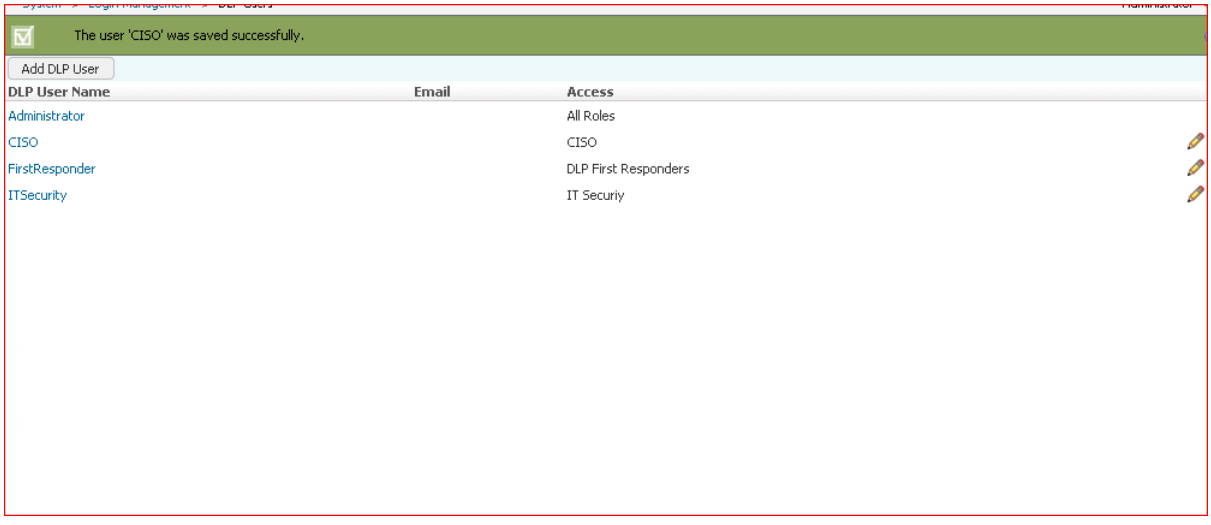
Adding the First Responder to the DLP USER



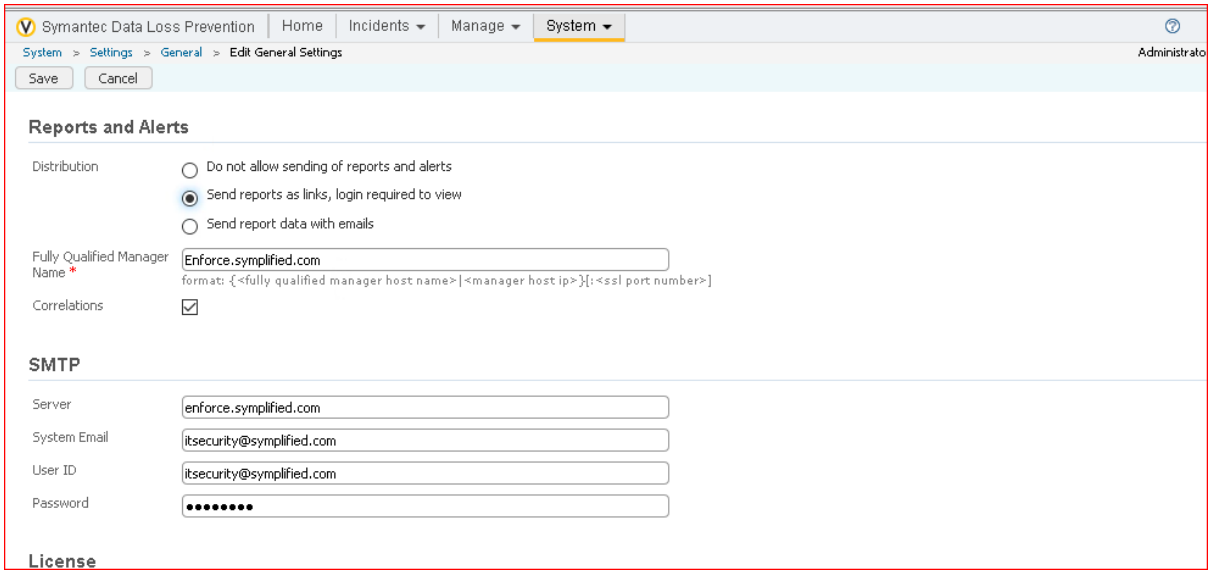
Adding the IT security team to the DLP USER



Adding the CISO team to the DLP USER



Displaying the teams added to the DLP USERS

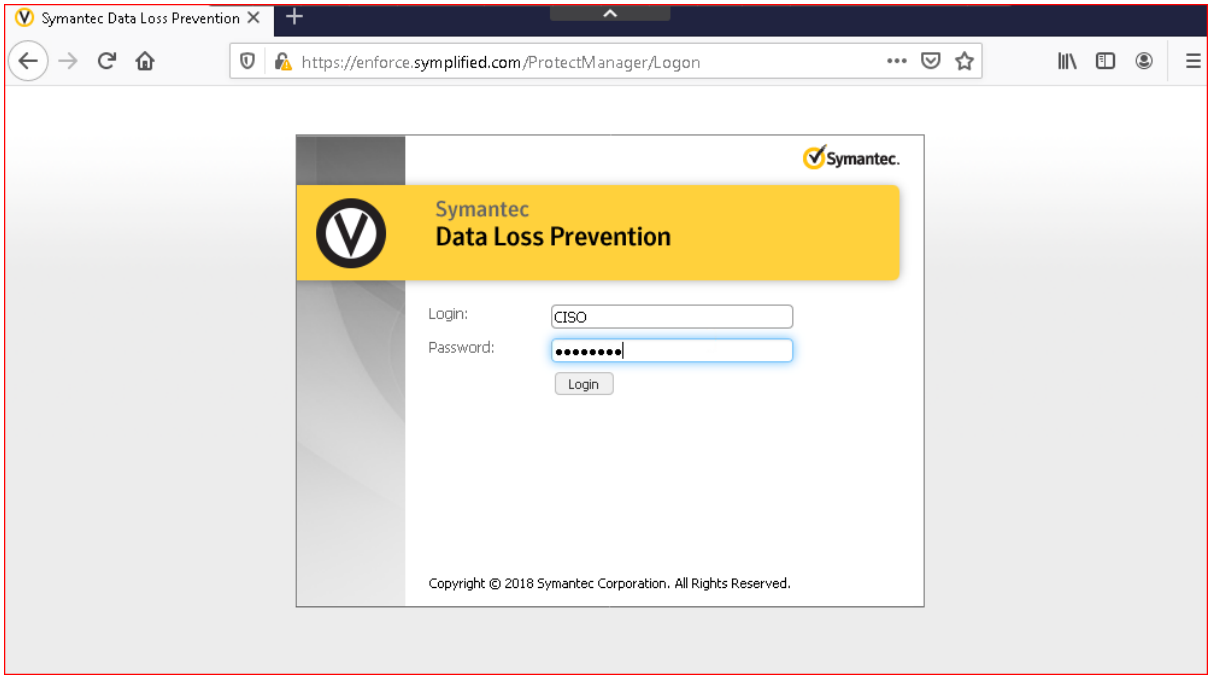


At last we are configuring the rules and we selected the option send reports as links, login required to view in Distribution tab.

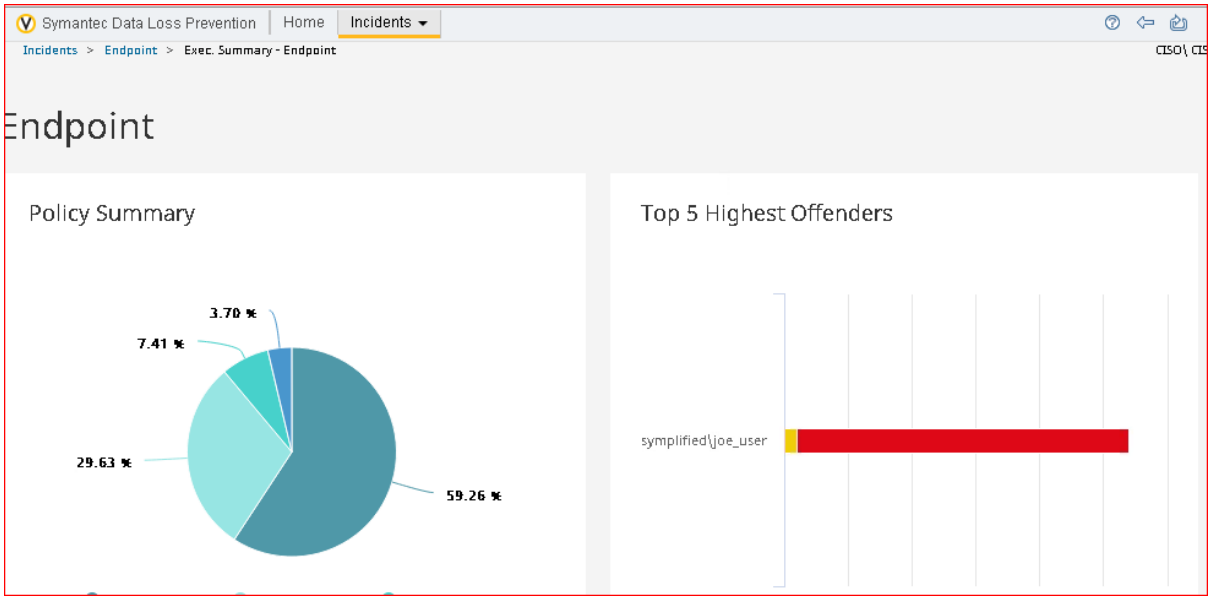
Exercise 2:

User reports to track risk Exposure and Reduction.

Generally the organization want to keep the data very secure and they will ask the proof of incidents to the Symantec DLP team and also asks how the daily implementation is going on. They also want to see that the data loss is reducing and they want that report. In order to provide that custom reports and custom dashboard need to be created in the Enforce Console. This enables the organization to view the real time reporting on data loss reduction.

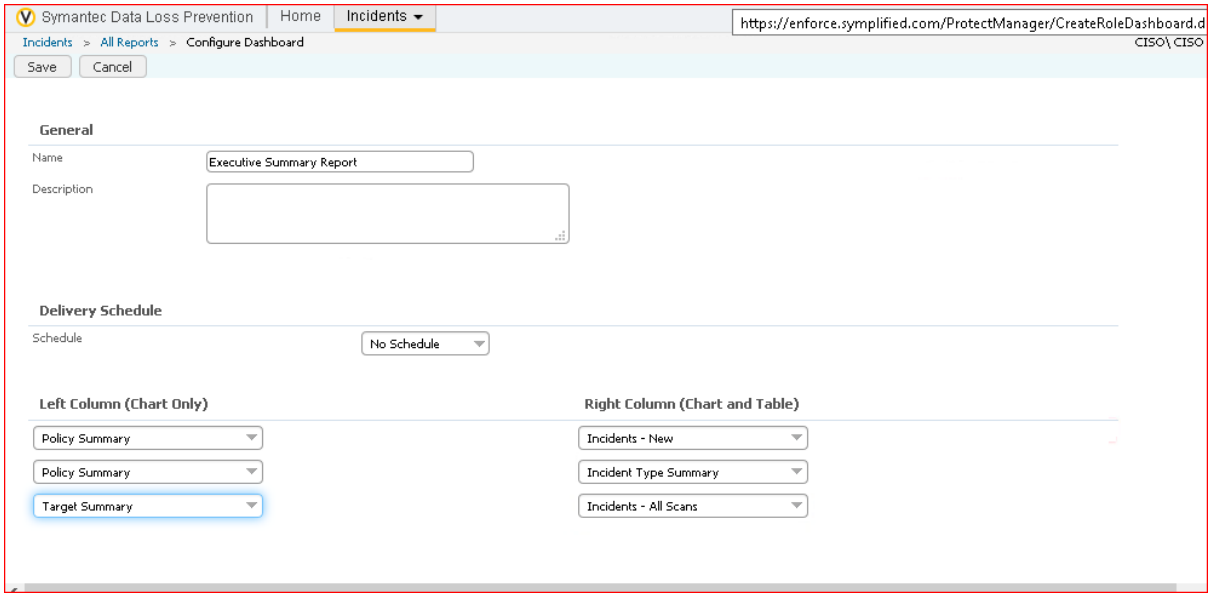


Login as CISO

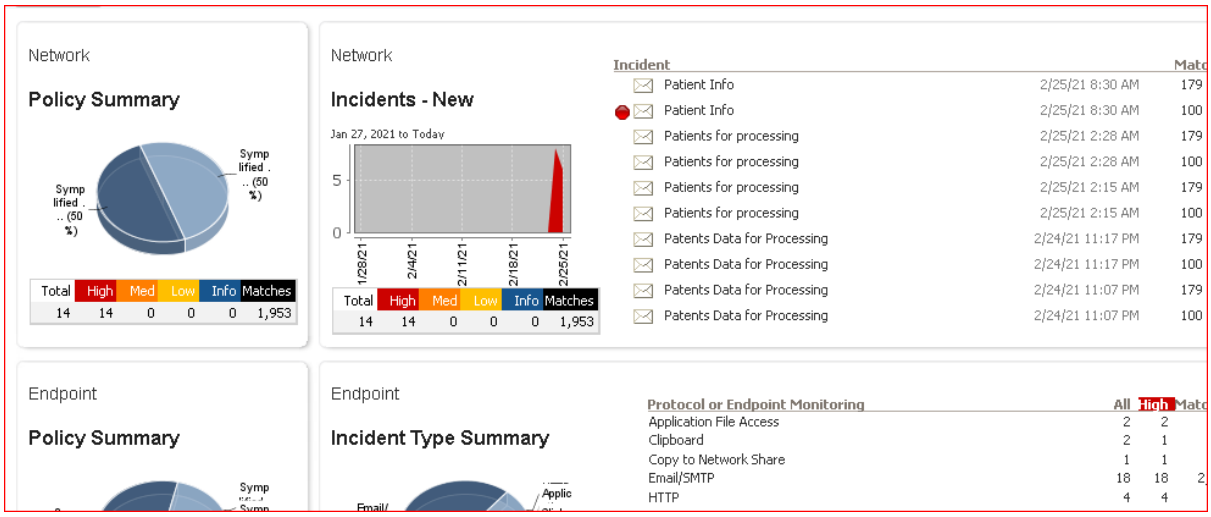


We can clearly see that no of options decreased when logging as CISO

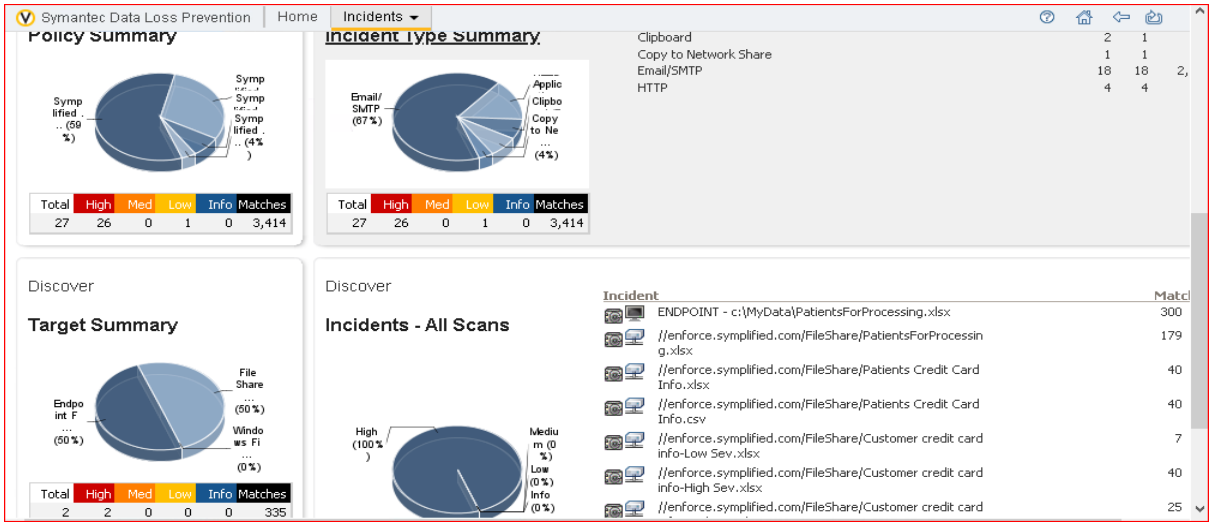
Vinay Kumar Reddy Donda dondavinayreddy@gmail.com



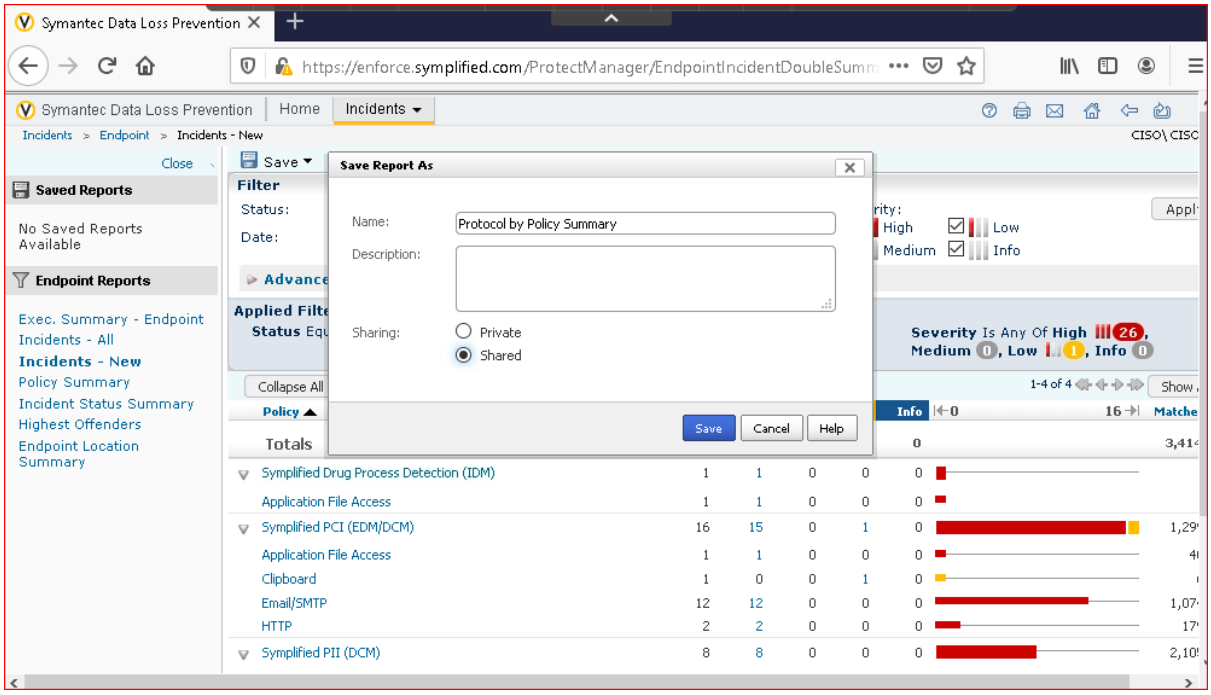
Generating the new report according to the needs



Displaying the saved reports



Displaying the saved report



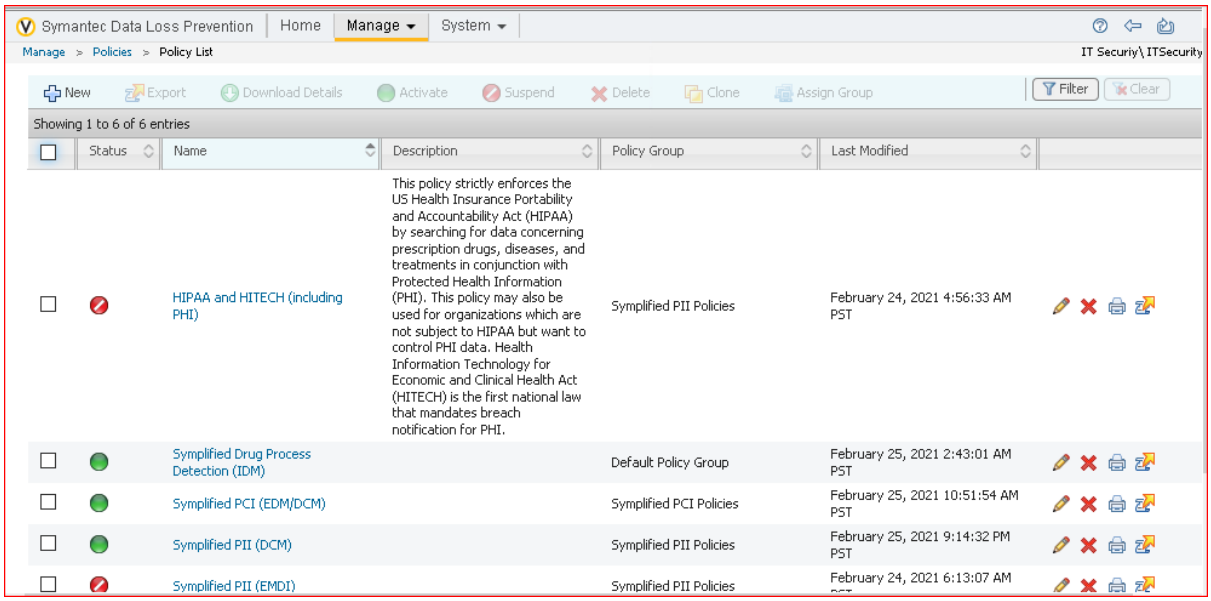
Generating the new report as Protocol by Policy Summary.

Vinay Kumar Reddy Donda dondavinayreddy@gmail.com

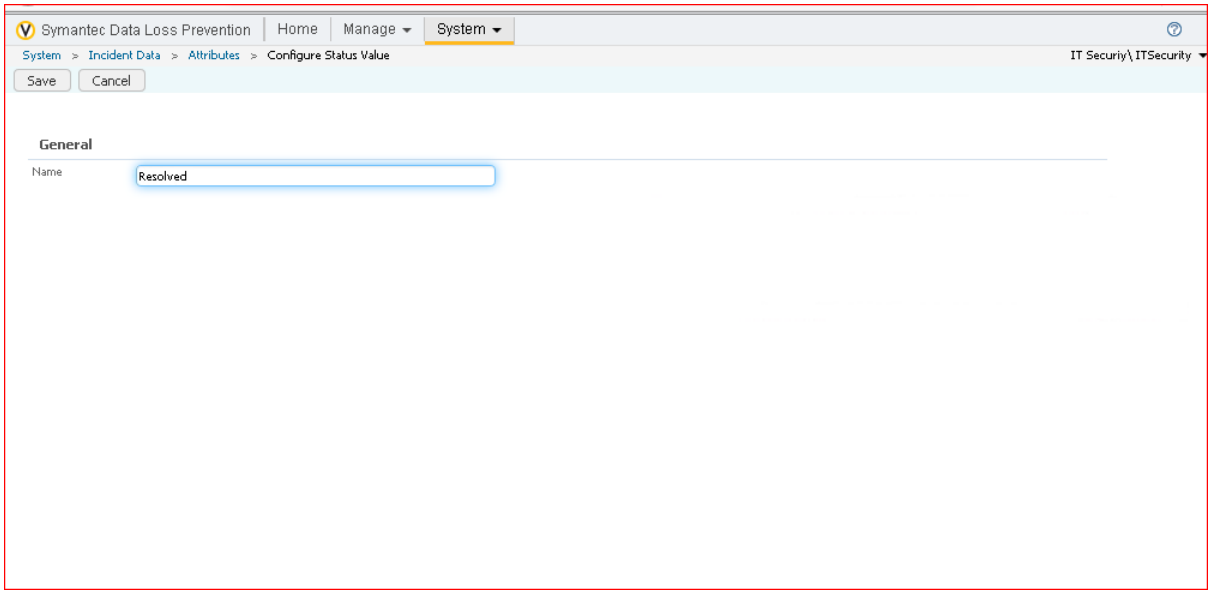
Exercise 3:

Define Incident statuses and incident groups.

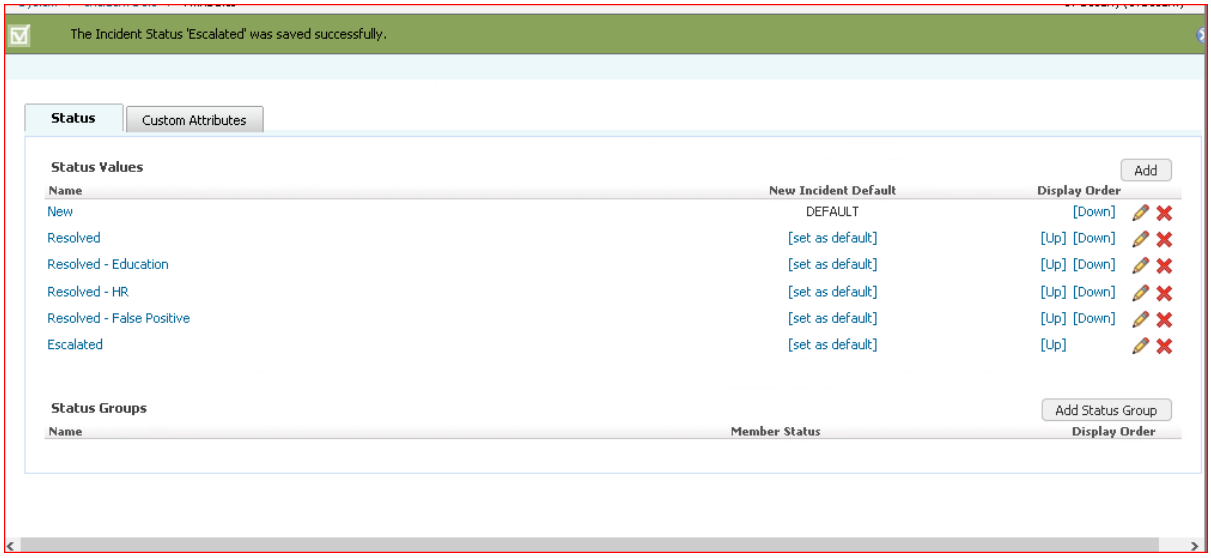
The first responders team within it department has expressed a need for some new incident statues to be created.These new statues will make it easier for the esclalation team to focus on the higher priority incidents first and help everyone keep track of which incidents have been already addressed.



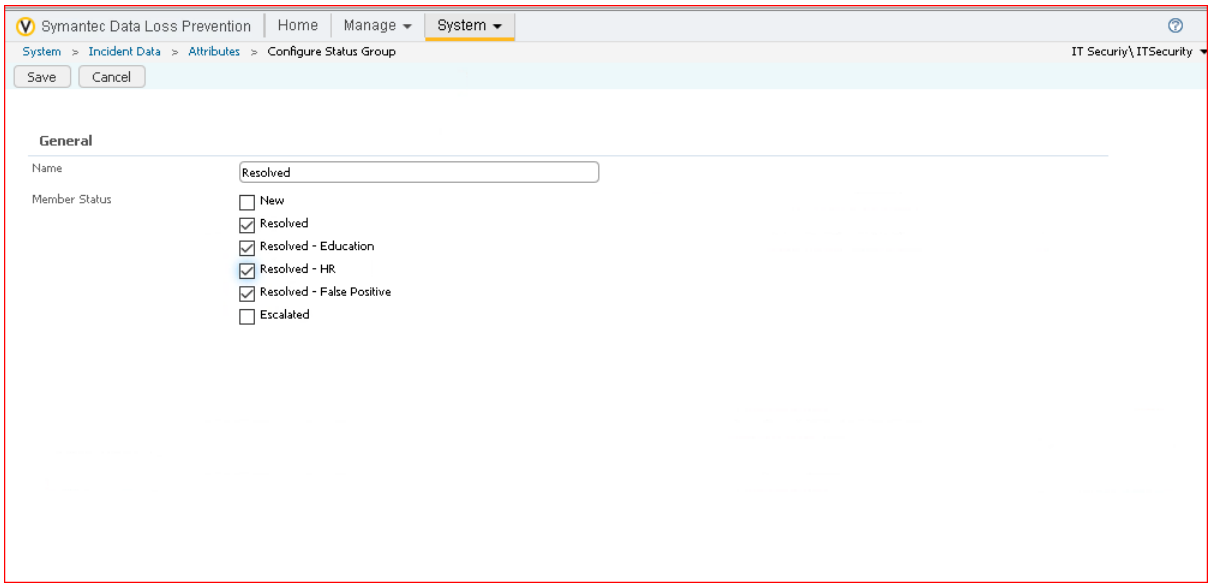
We can see there is no incident tab when we logged in as the IT Security team.



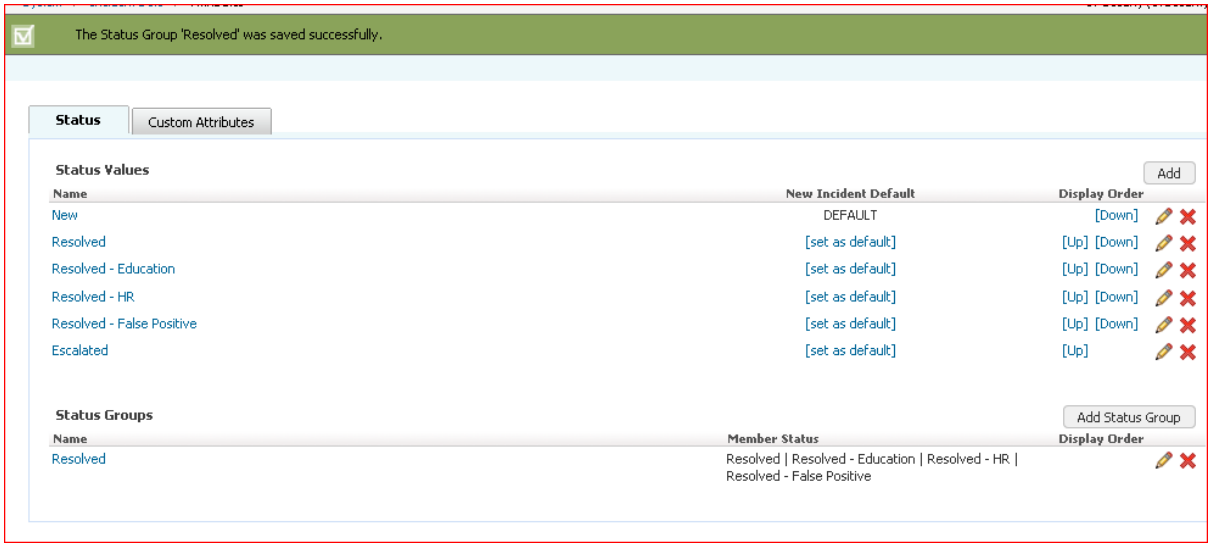
Configuring the status value



Configured the status values



Configuring the status group.

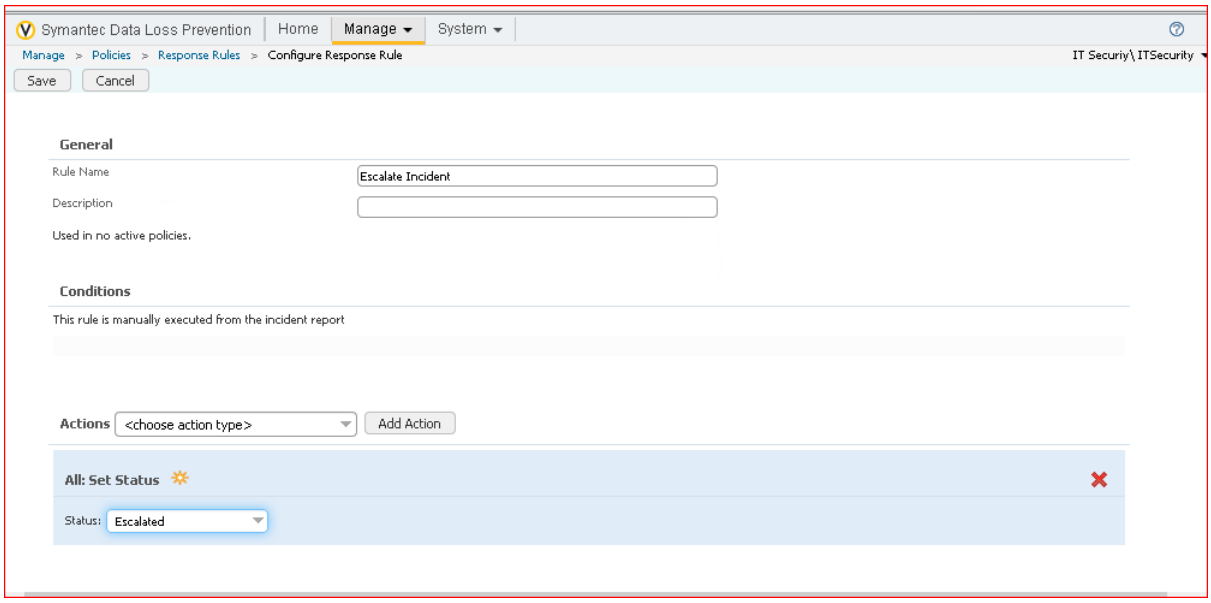


Displaying all the status groups and status values.

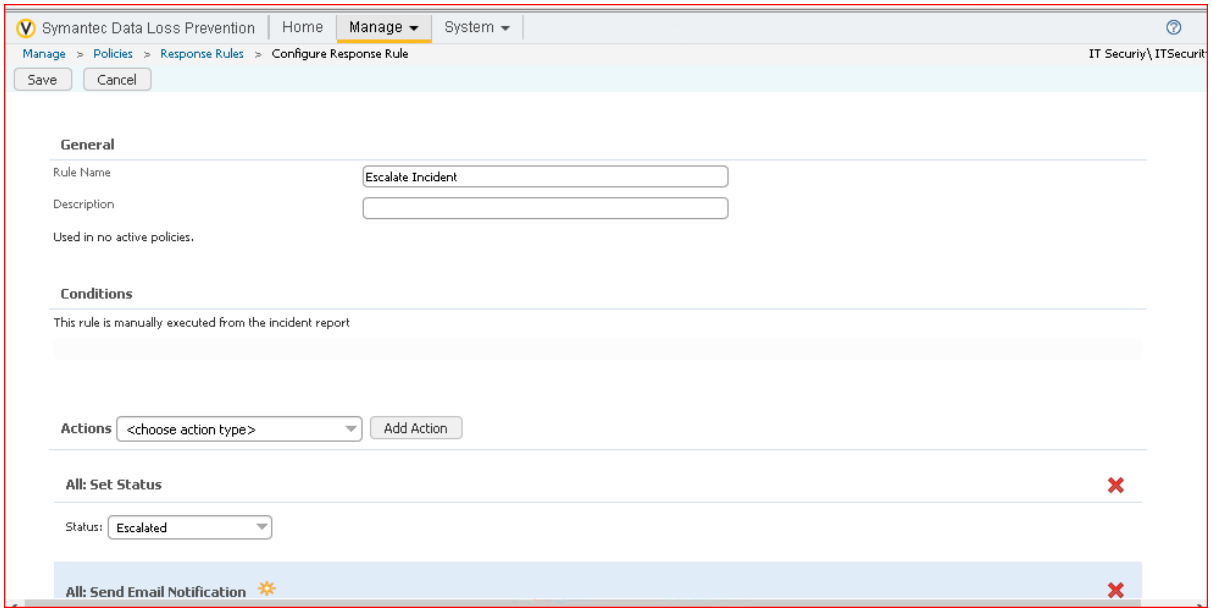
Vinay Kumar Reddy Donda dondavinayreddy@gmail.com

Exercise 4:
Configure and Use smart responses:

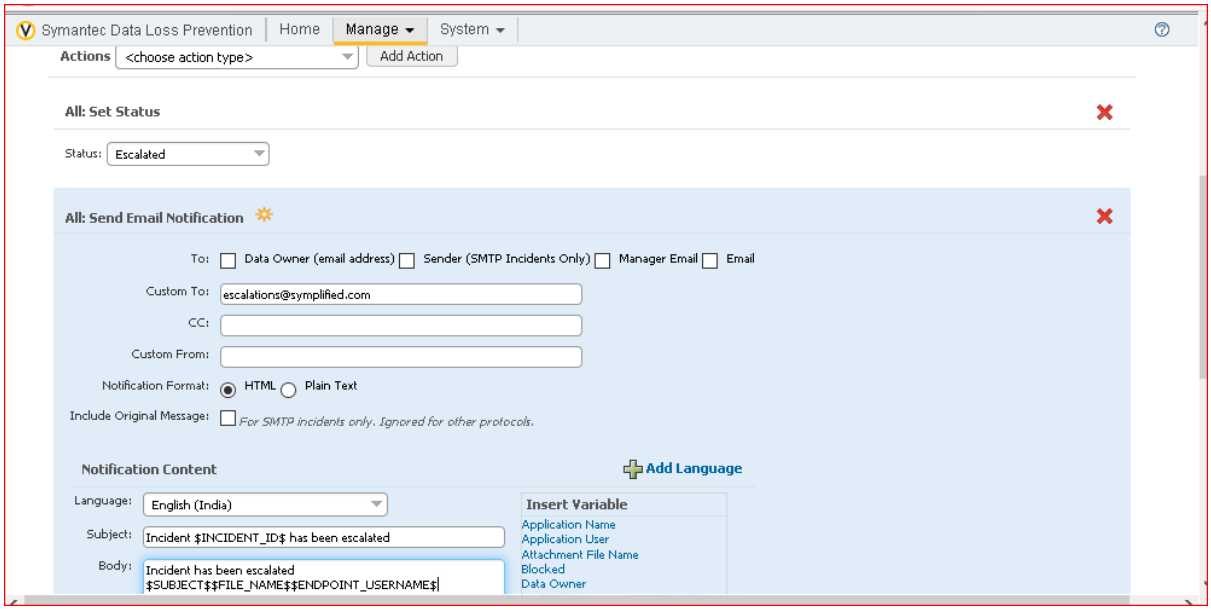
Generally the first responders team has been manually changing the status of the incidents they review to “Escalated” or “Resolved-Education” depending upon the type of the incident but this is taking too much time so upon investigating the it team has come up with the smart responses that will help speed up the process of changing the incident status and sending out any notification emails to users or managers.



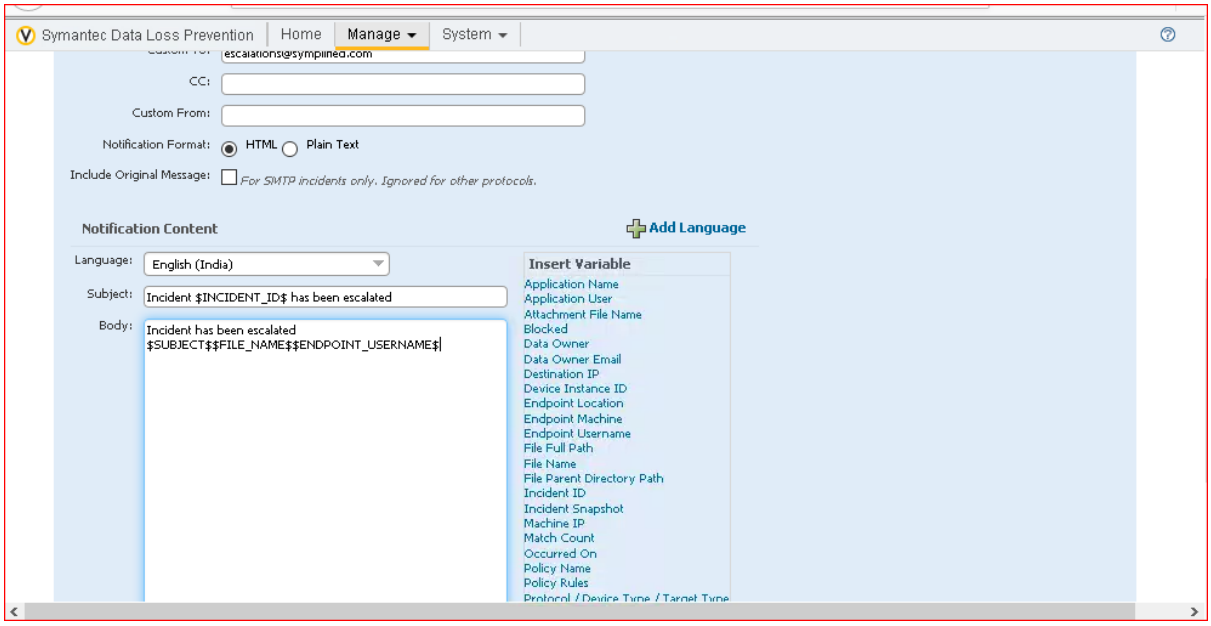
Adding the response rules



Adding the response rules

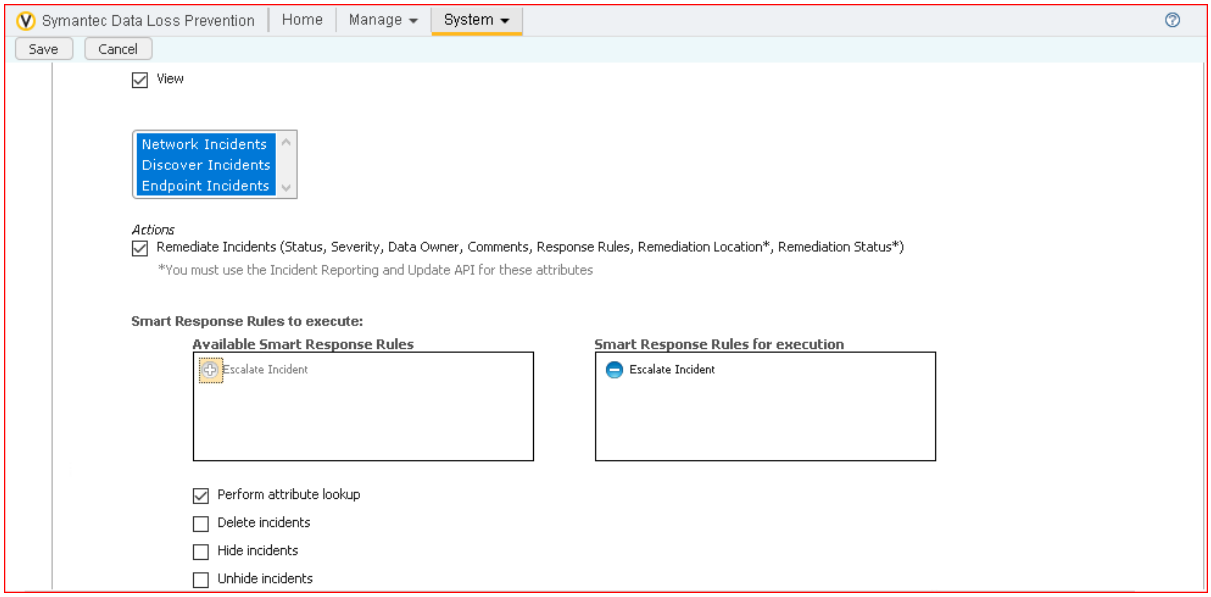


Adding the response rules

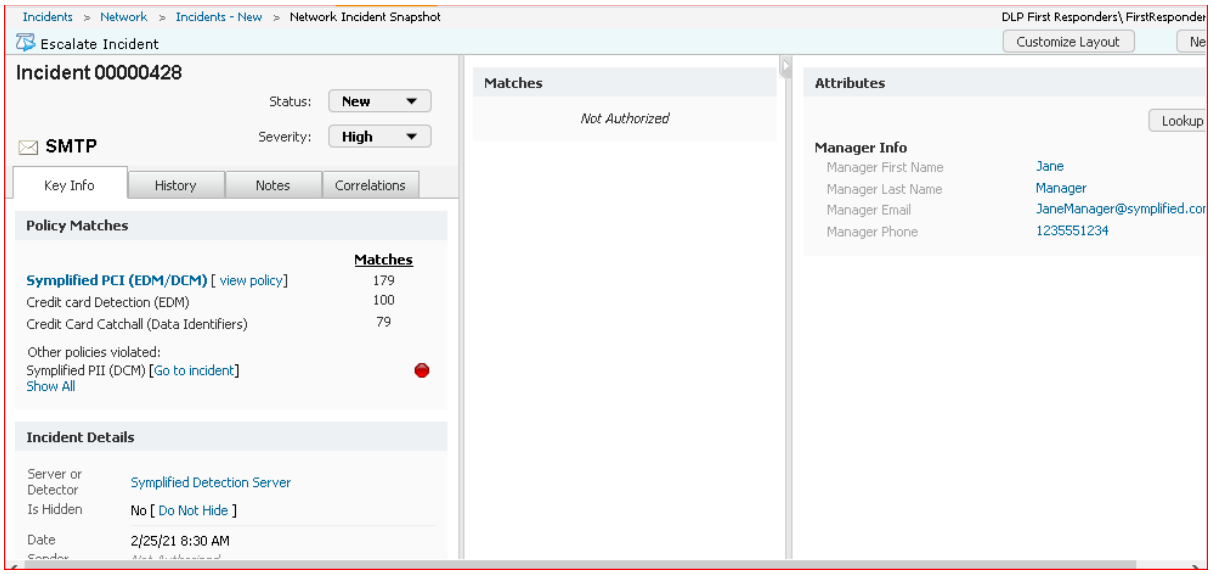


Adding the response rules

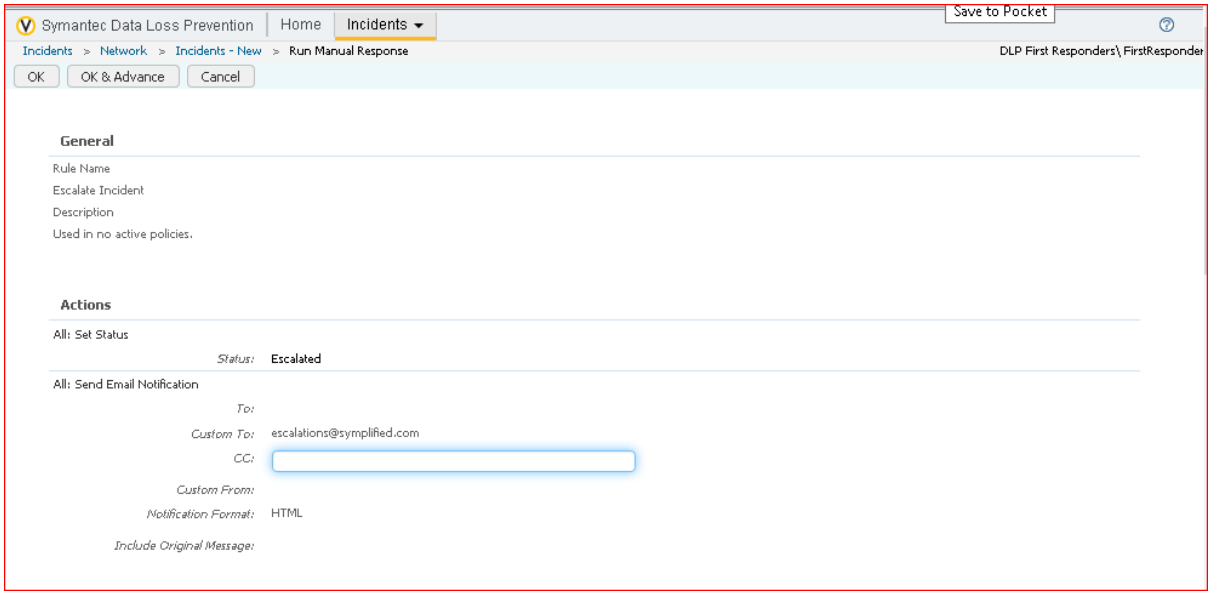
Vinay Kumar Reddy Donda dondavinayreddy@gmail.com



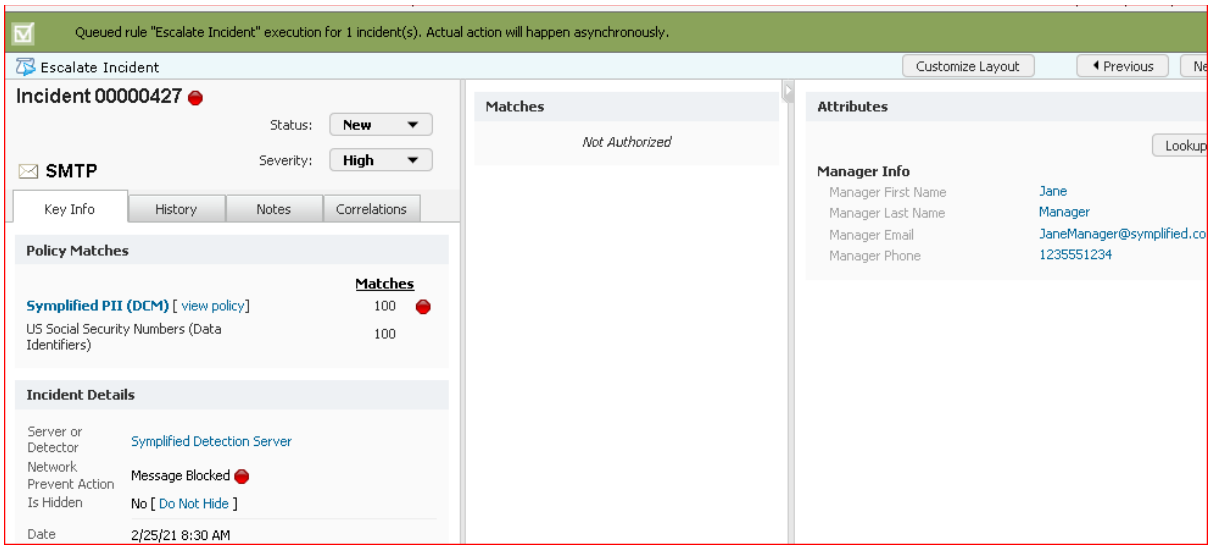
Adding the escalate incident option



Processing of escalating



Clicked on OK&Advance and proceed

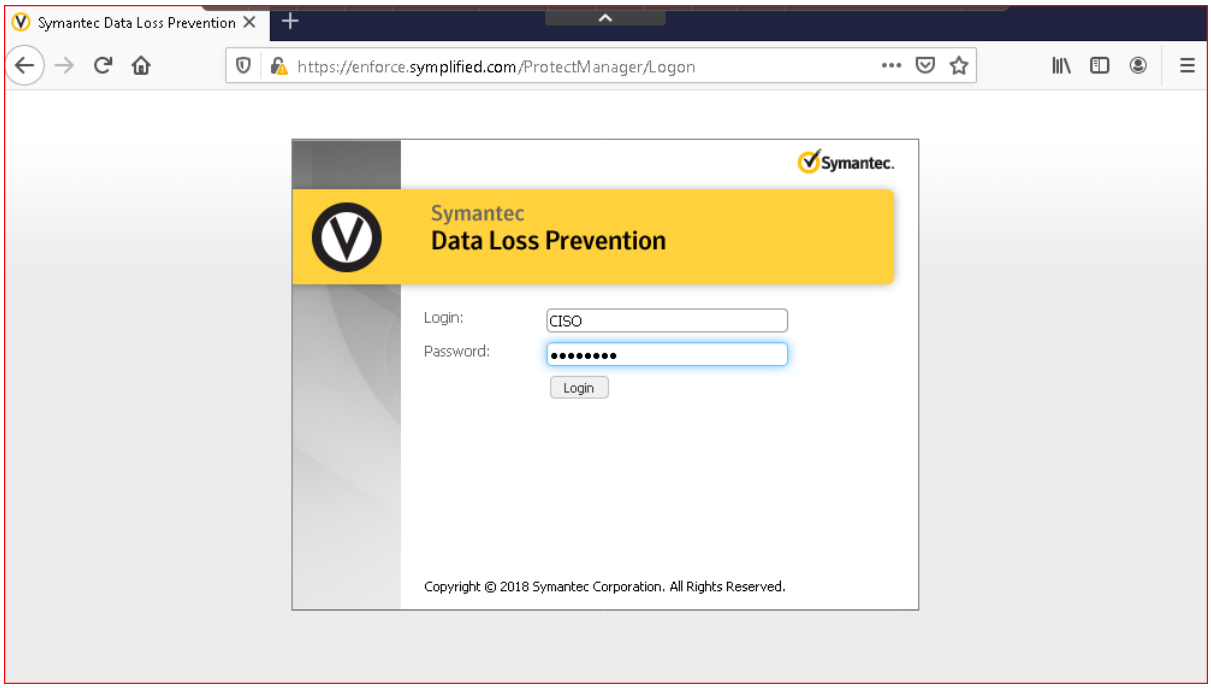


We can see that incident is escalated.

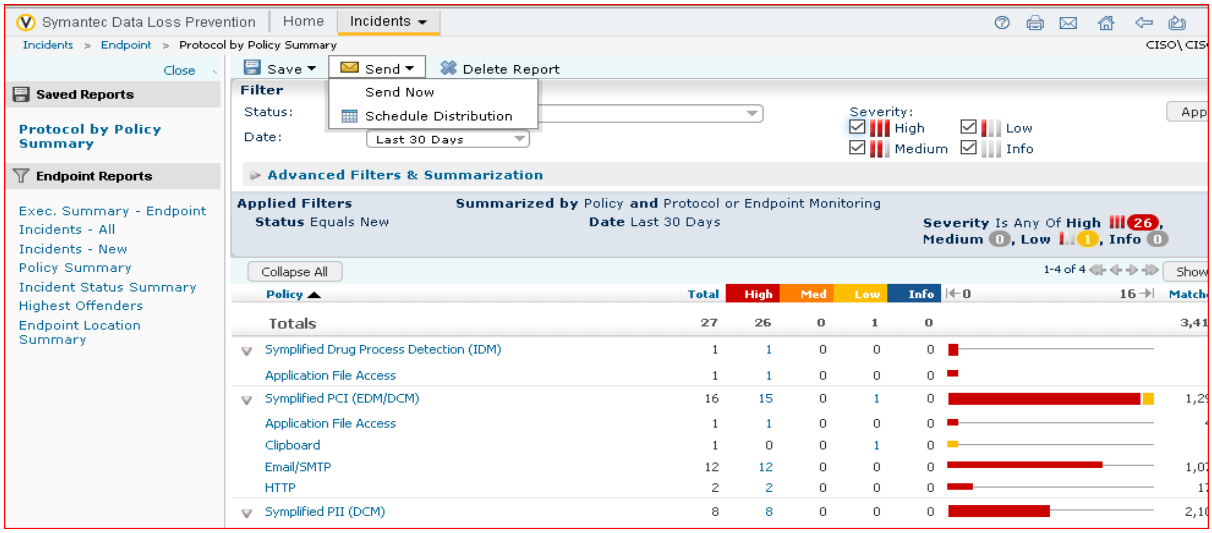
Exercise 5:

Schedule and send reports.

The organizational requested to submit the reports automatically on monlthy basis. This makes easy to look after the data although the employees can login and see the reports but since they are busy and the report will be sent to the mails directly.

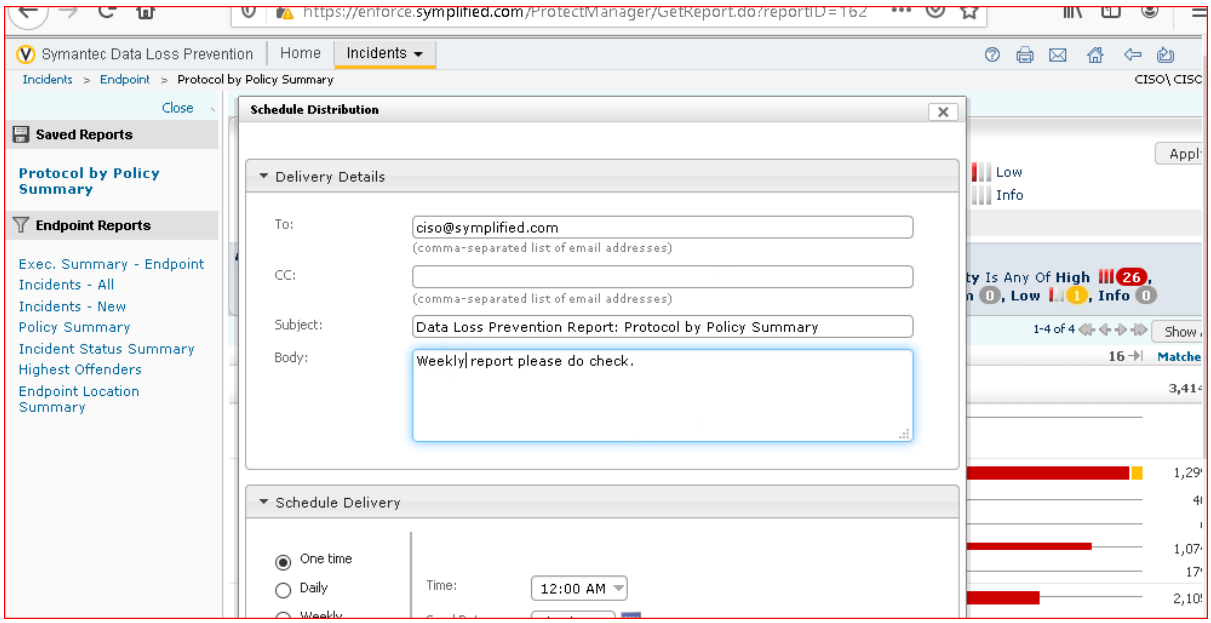


Login through CISO

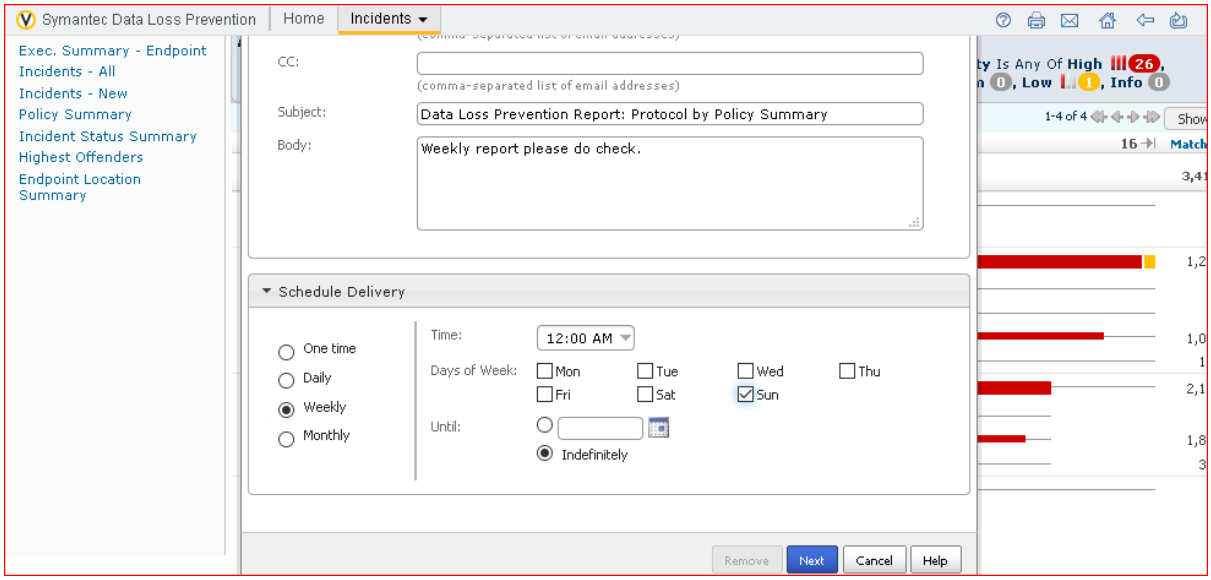


On the top we can see that We can Schedule the distribution.

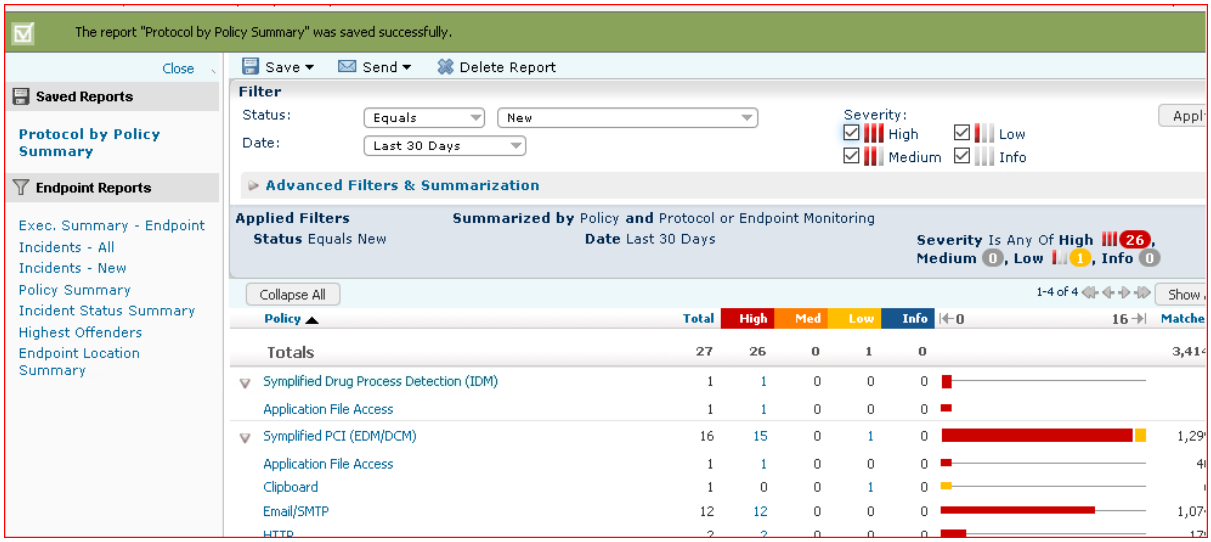
Vinay Kumar Reddy Donda dondavinayreddy@gmail.com



We need to add the details



Weekly report and should send on the sunday



Confirmation that the report will be sent weekly.

Section 7:

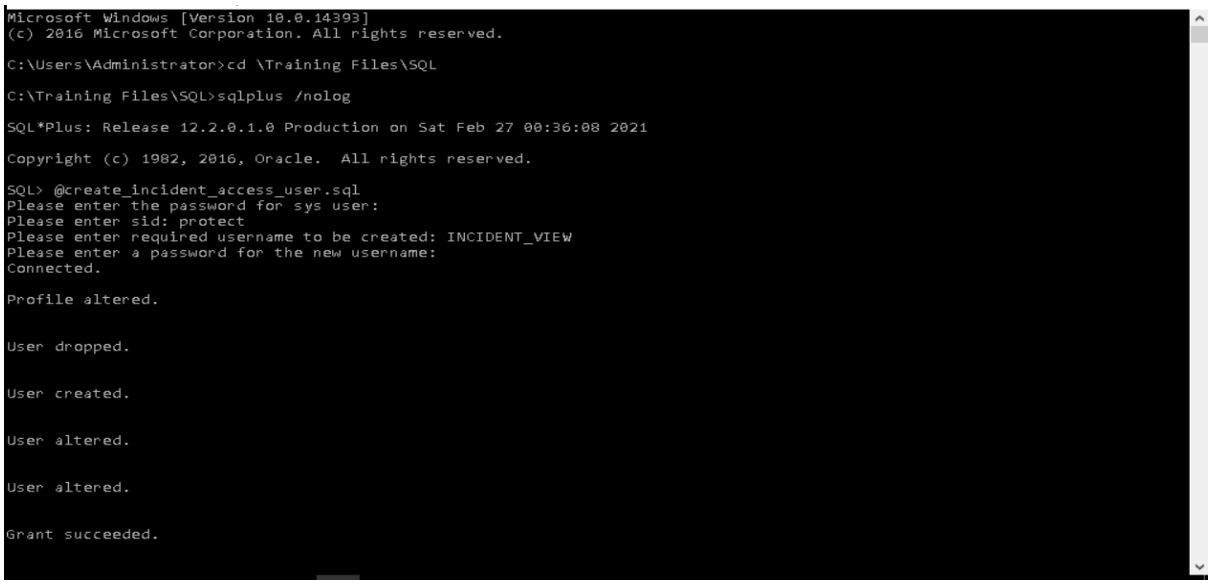
Enhancing data loss preventions with Integrations.

In this labs we will look at the additional products and tools that integrate with the Symantec dlp and how this products and tools assist in the goal of finding and protecting confidential and sensitive data.

Exercise 1:

Create the views schema and user.

Though the reporting features are very useful and powerful, there are times when highly specialized report is required. Using the incident data views, it is possible to use SQl Queries to create the custom report to fit nearly every reporting need.



Steps for executing this exercise

Executed successfully and Disconnected from the oracle database.

Exercise 2:

Run the Incident data view steup script.

After the incident data view user is configured, a setup script is run to create the actual incident data views in the oracle database.

```
C:\Training Files\SQL>sqlplus /nolog

SQL*Plus: Release 12.2.0.1.0 Production on Sat Feb 27 01:00:23 2021

Copyright (c) 1982, 2016, Oracle.  All rights reserved.

SQL> @setup.sql
Please enter sid: protect
Please enter username for the Enforce schema: protect
Please enter password for the Enforce schema:
Please enter username for the Incident Access schema: INCIDENT_VIEW
Please enter password for the Incident Access schema:
Connected.
old   1: GRANT SELECT ON INCIDENT TO &view_username
new   1: GRANT SELECT ON INCIDENT TO INCIDENT_VIEW

Grant succeeded.

old   1: GRANT SELECT ON MESSAGE TO &view_username
new   1: GRANT SELECT ON MESSAGE TO INCIDENT_VIEW

Grant succeeded.

old   1: GRANT SELECT ON MESSAGECOMPONENT TO &view_username
new   1: GRANT SELECT ON MESSAGECOMPONENT TO INCIDENT_VIEW

Grant succeeded.

old   1: GRANT SELECT ON MESSAGEORIGINATOR TO &view_username
new   1: GRANT SELECT ON MESSAGEORIGINATOR TO INCIDENT_VIEW
```

Process of running the setup script

```
Please enter sid: protect
Please enter username for the Enforce schema: protect
Please enter password for the Enforce schema:
Please enter username for the Incident Access schema: INCIDENT_VIEW
Please enter password for the Incident Access schema:
Connected.
old   1: GRANT SELECT ON INCIDENT TO &view_username
new   1: GRANT SELECT ON INCIDENT TO INCIDENT_VIEW

Grant succeeded.

old   1: GRANT SELECT ON MESSAGE TO &view_username
new   1: GRANT SELECT ON MESSAGE TO INCIDENT_VIEW

Grant succeeded.

old   1: GRANT SELECT ON MESSAGECOMPONENT TO &view_username
new   1: GRANT SELECT ON MESSAGECOMPONENT TO INCIDENT_VIEW

Grant succeeded.

old   1: GRANT SELECT ON MESSAGEORIGINATOR TO &view_username
new   1: GRANT SELECT ON MESSAGEORIGINATOR TO INCIDENT_VIEW

Grant succeeded.

old   1: GRANT SELECT ON MESSAGERECIPIENT TO &view_username
new   1: GRANT SELECT ON MESSAGERECIPIENT TO INCIDENT_VIEW

Grant succeeded.

old   1: GRANT SELECT ON MESSAGEACLENTRY TO &view_username
new   1: GRANT SELECT ON MESSAGEACLENTRY TO INCIDENT_VIEW

Grant succeeded.
```

Result after executing the setup queries

```
old   1: GRANT SELECT ON SCANASSIGNMENT TO &view_username
new   1: GRANT SELECT ON SCANASSIGNMENT TO INCIDENT_VIEW

Grant succeeded.

old   1: GRANT SELECT ON INFORMATIONMONITOR TO &view_username
new   1: GRANT SELECT ON INFORMATIONMONITOR TO INCIDENT_VIEW

Grant succeeded.

old   1: GRANT SELECT ON POLICY TO &view_username
new   1: GRANT SELECT ON POLICY TO INCIDENT_VIEW

Grant succeeded.

old   1: GRANT SELECT ON POLICYGROUP TO &view_username
new   1: GRANT SELECT ON POLICYGROUP TO INCIDENT_VIEW

Grant succeeded.

old   1: GRANT SELECT ON DATAOWNER TO &view_username
new   1: GRANT SELECT ON DATAOWNER TO INCIDENT_VIEW

Grant succeeded.

old   1: GRANT SELECT ON DATAOWNEREMAIL TO &view_username
new   1: GRANT SELECT ON DATAOWNEREMAIL TO INCIDENT_VIEW

Grant succeeded.

old   1: GRANT SELECT ON INCIDENTSTATUS TO &view_username
new   1: GRANT SELECT ON INCIDENTSTATUS TO INCIDENT_VIEW

Grant succeeded.

old   1: GRANT SELECT ON CONDITIONVIEW TO &view_username
```

Result which shows us old and new views

```
Synonym created.

old   1: CREATE OR REPLACE SYNONYM SCANASSIGNMENT FOR &enforce_username..SCANASSIGNMENT
new   1: CREATE OR REPLACE SYNONYM SCANASSIGNMENT FOR protect.SCANASSIGNMENT

Synonym created.

old   1: CREATE OR REPLACE SYNONYM INFORMATIONMONITOR FOR &enforce_username..INFORMATIONMONITOR
new   1: CREATE OR REPLACE SYNONYM INFORMATIONMONITOR FOR protect.INFORMATIONMONITOR

Synonym created.

old   1: CREATE OR REPLACE SYNONYM POLICY FOR &enforce_username..POLICY
new   1: CREATE OR REPLACE SYNONYM POLICY FOR protect.POLICY

Synonym created.

old   1: CREATE OR REPLACE SYNONYM POLICYGROUP FOR &enforce_username..POLICYGROUP
new   1: CREATE OR REPLACE SYNONYM POLICYGROUP FOR protect.POLICYGROUP

Synonym created.

old   1: CREATE OR REPLACE SYNONYM DATAOWNER FOR &enforce_username..DATAOWNER
new   1: CREATE OR REPLACE SYNONYM DATAOWNER FOR protect.DATAOWNER

Synonym created.

old   1: CREATE OR REPLACE SYNONYM DATAOWNEREMAIL FOR &enforce_username..DATAOWNEREMAIL
new   1: CREATE OR REPLACE SYNONYM DATAOWNEREMAIL FOR protect.DATAOWNEREMAIL

Synonym created.

old   1: CREATE OR REPLACE SYNONYM INCIDENTSTATUS FOR &enforce_username..INCIDENTSTATUS
new   1: CREATE OR REPLACE SYNONYM INCIDENTSTATUS FOR protect.INCIDENTSTATUS

Synonym created.
```

Result which shows the old and new views

View created and disconnect from the oracle database

Exercise 3:

Verify Incident Data Views Creation

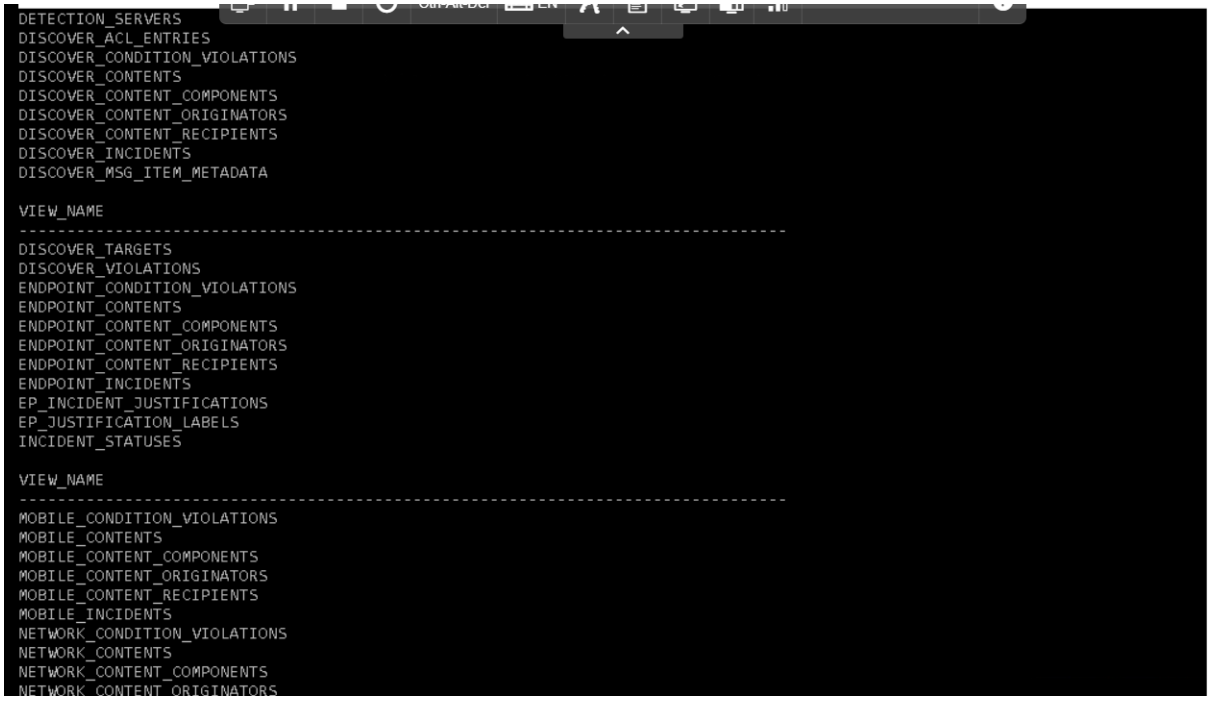
After running the user creation setup scripts, it is important to verify that the incident data views were created successfully.

```
View created.

View created.

View created.

View created.

View created.

View created.

View created.

Disconnected from Oracle Database 12c Standard Edition Release 12.2.0.1.0 - 64bit Production

C:\Training Files\SQL>sqlplus INCIDENT_VIEW/INCIDENT_VIEW@PROTECT

SQL*Plus: Release 12.2.0.1.0 Production on Sat Feb 27 01:10:52 2021

Copyright (c) 1982, 2016, Oracle.  All rights reserved.

Last Successful login time: Sat Feb 27 2021 01:01:22 -08:00

Connected to:
Oracle Database 12c Standard Edition Release 12.2.0.1.0 - 64bit Production
```

Verifying whether the incident data views are created or not

```
Copyright (c) 1982, 2016, Oracle.  All rights reserved.

Last Successful login time: Sat Feb 27 2021 01:01:22 -08:00

Connected to:
Oracle Database 12c Standard Edition Release 12.2.0.1.0 - 64bit Production

SQL> select VIEW_NAME from USER_VIEWS;

VIEW_NAME
--------------------------------------------------------------------------------
CUSTOM_ATTRIBUTES
CUSTOM_ATTRIBUTE_DEFINITIONS
DETECTION_SERVERS
DISCOVER_ACL_ENTRIES
DISCOVER_CONDITION_VIOLATIONS
DISCOVER_CONTENTS
DISCOVER_CONTENT_COMPONENTS
DISCOVER_CONTENT_ORIGINATORS
DISCOVER_CONTENT_RECIPIENTS
DISCOVER_INCIDENTS
DISCOVER_MSG_ITEM_METADATA

VIEW_NAME
--------------------------------------------------------------------------------
DISCOVER_TARGETS
DISCOVER_VIOLATIONS
ENDPOINT_CONDITION_VIOLATIONS
ENDPOINT_CONTENTS
ENDPOINT_CONTENT_COMPONENTS
ENDPOINT_CONTENT_ORIGINATORS
ENDPOINT_CONTENT_RECIPIENTS
ENDPOINT_INCIDENTS
```

Displaying the different views



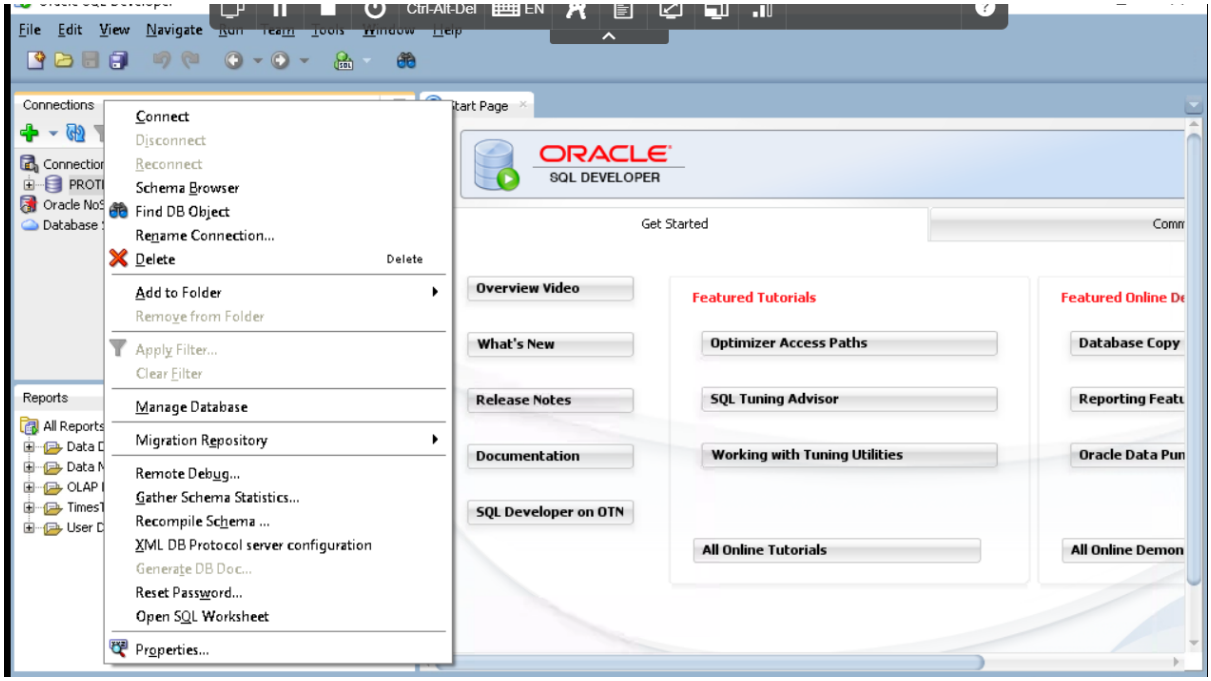
Displaying the different views

Displaying the different views

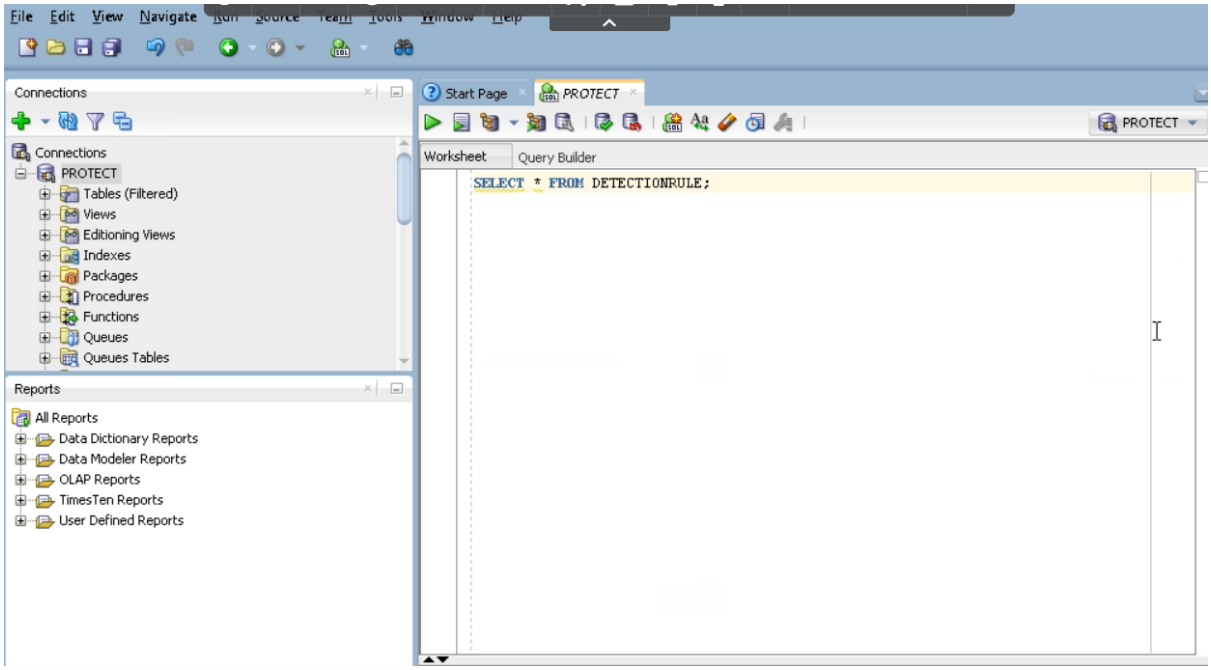
Exercise 4:

After successfully executing the user creation and set up scripts and verifying that the views are working, it is time to query the database using the incident data views.

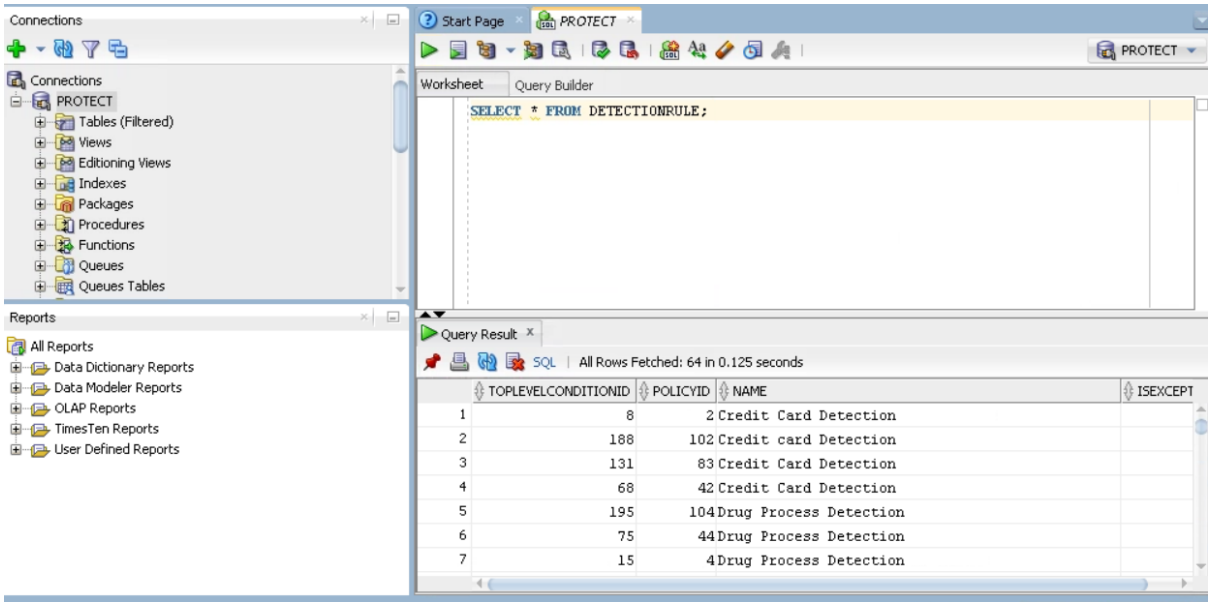
Incident data views enable the administrator to produce highly customized report by using the configured views and sql queries. Due to the complexity of this query , a few queries have been created which saves the time



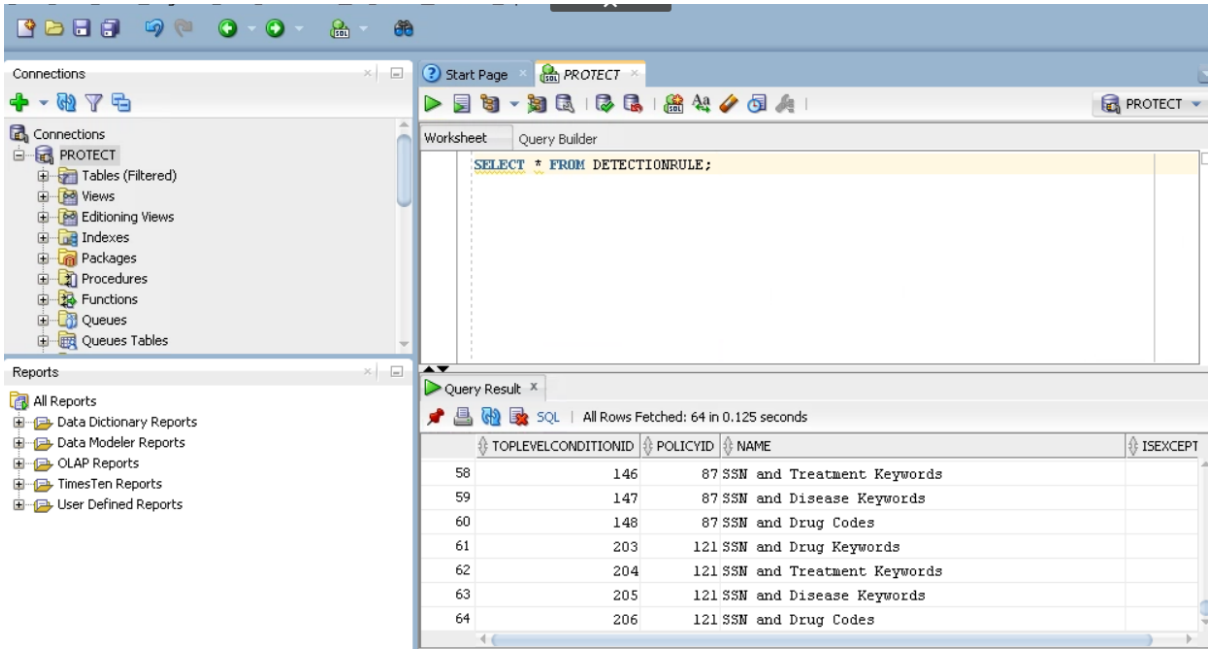
Connecting to the protect.



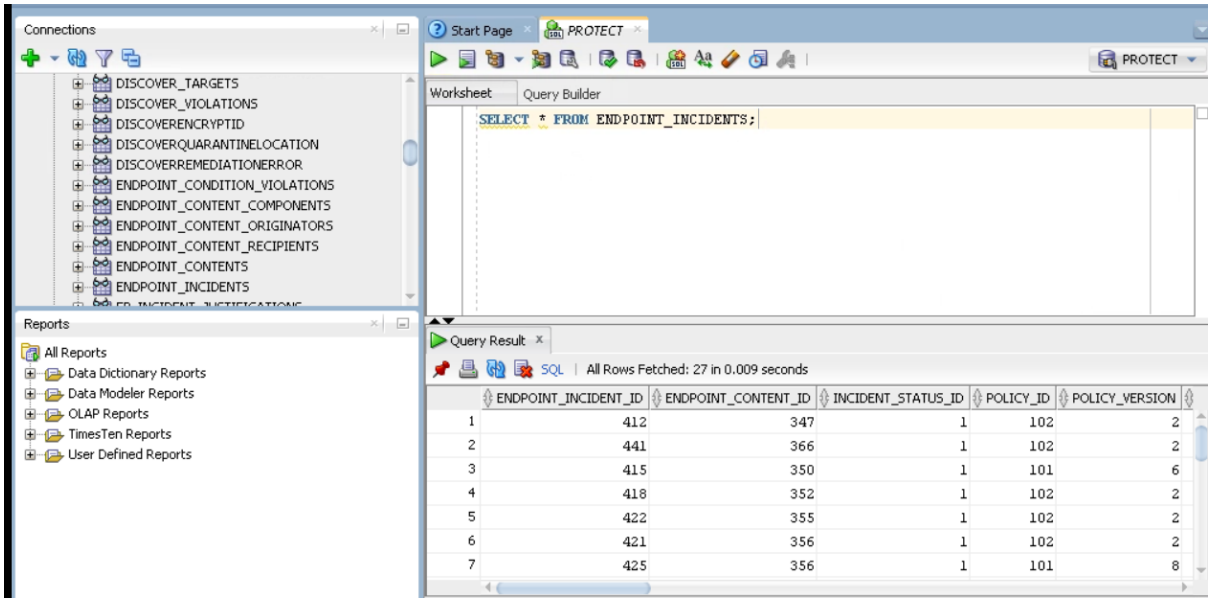
Connected and executing the query



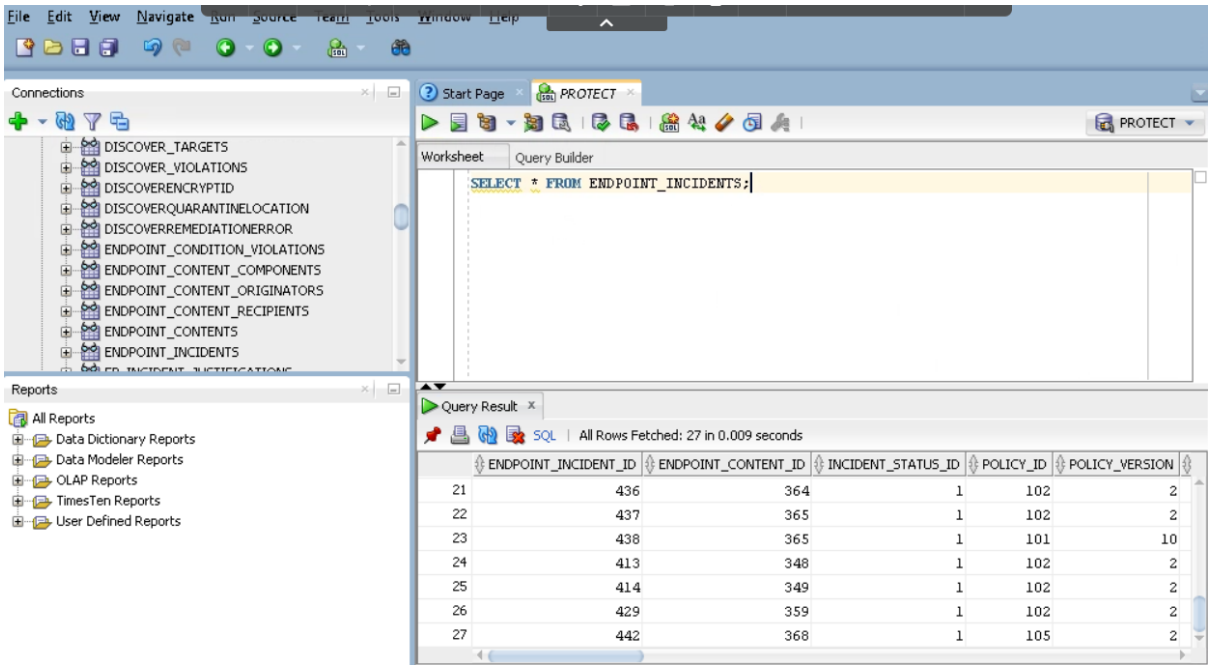
Result after executing the query.



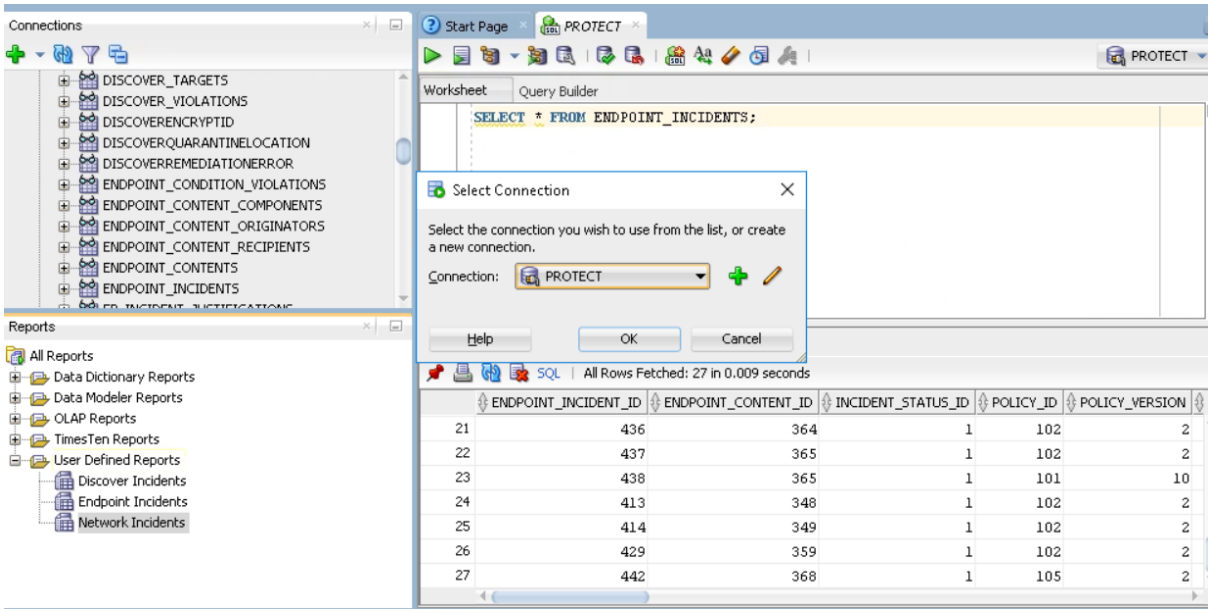
Result after executing the query



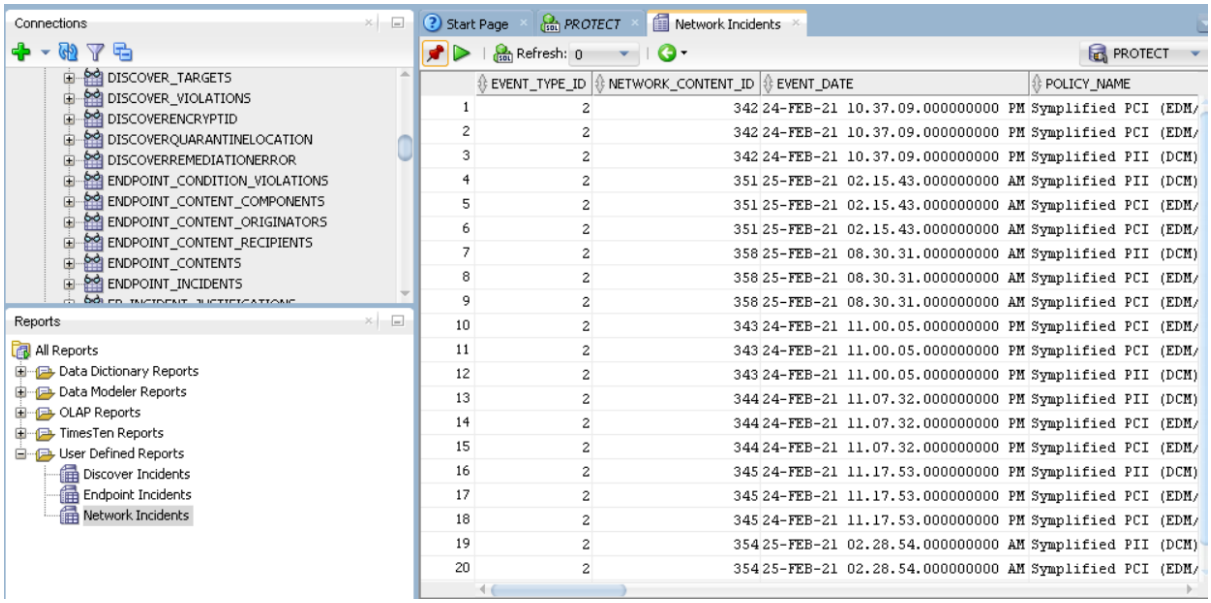
Result after executing the query on endpoint.



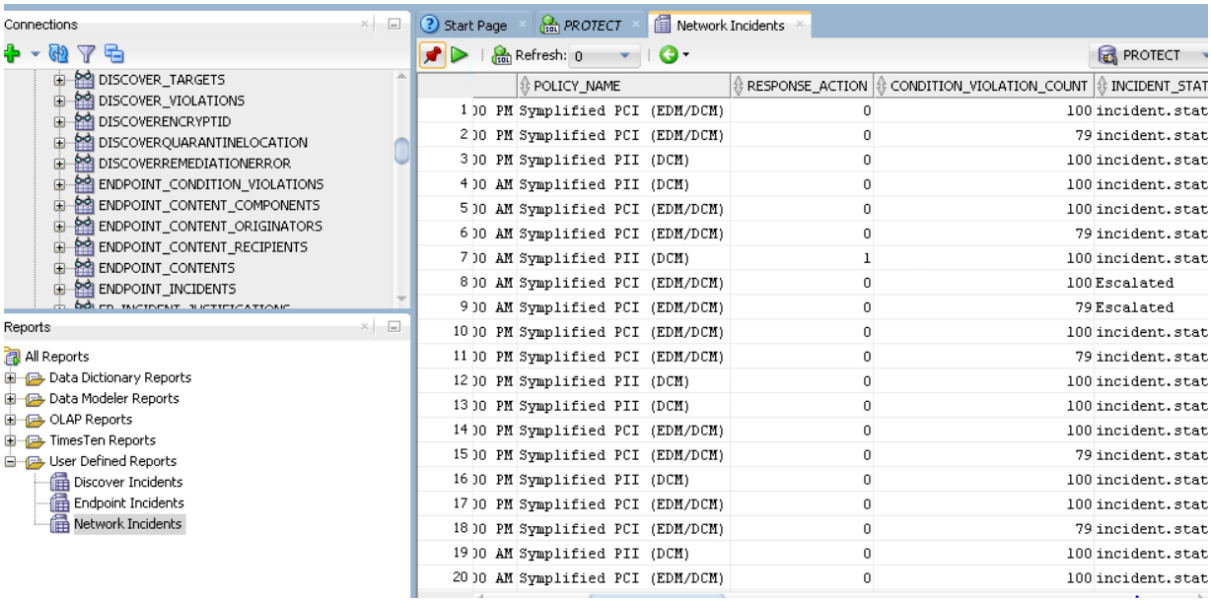
Result after executing the query



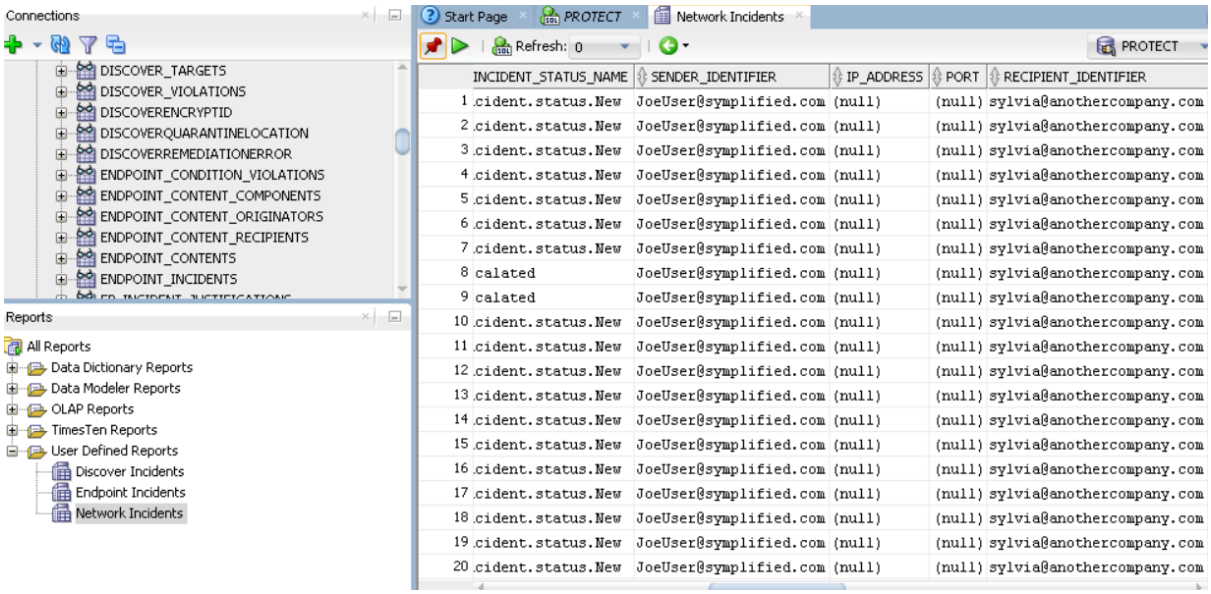
Process in order to display the network incidents.



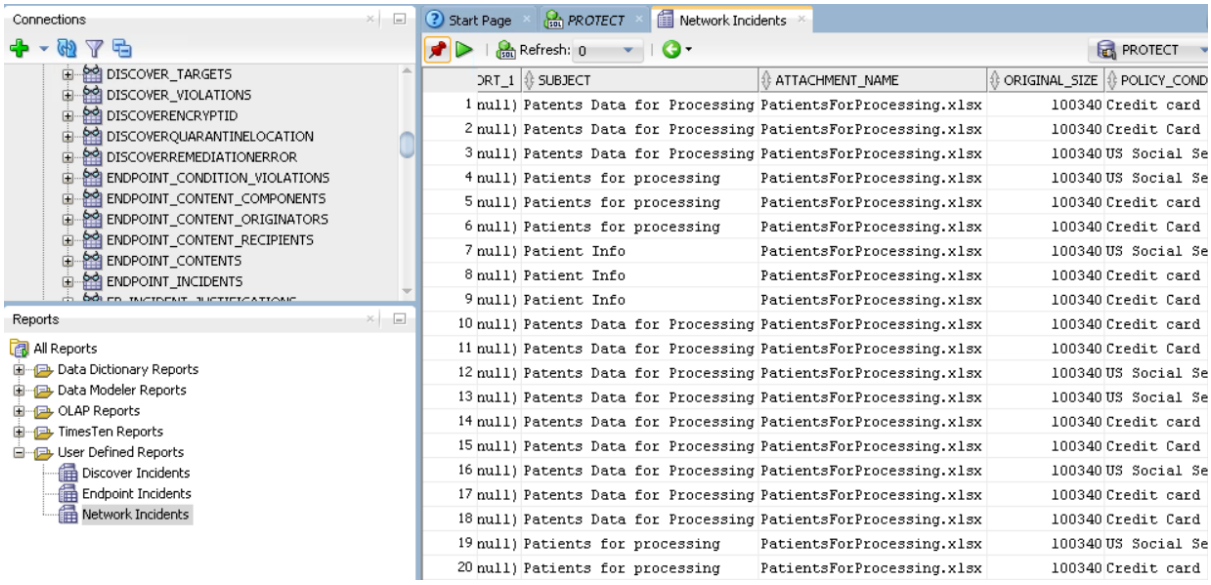
Displaying the network incidents.



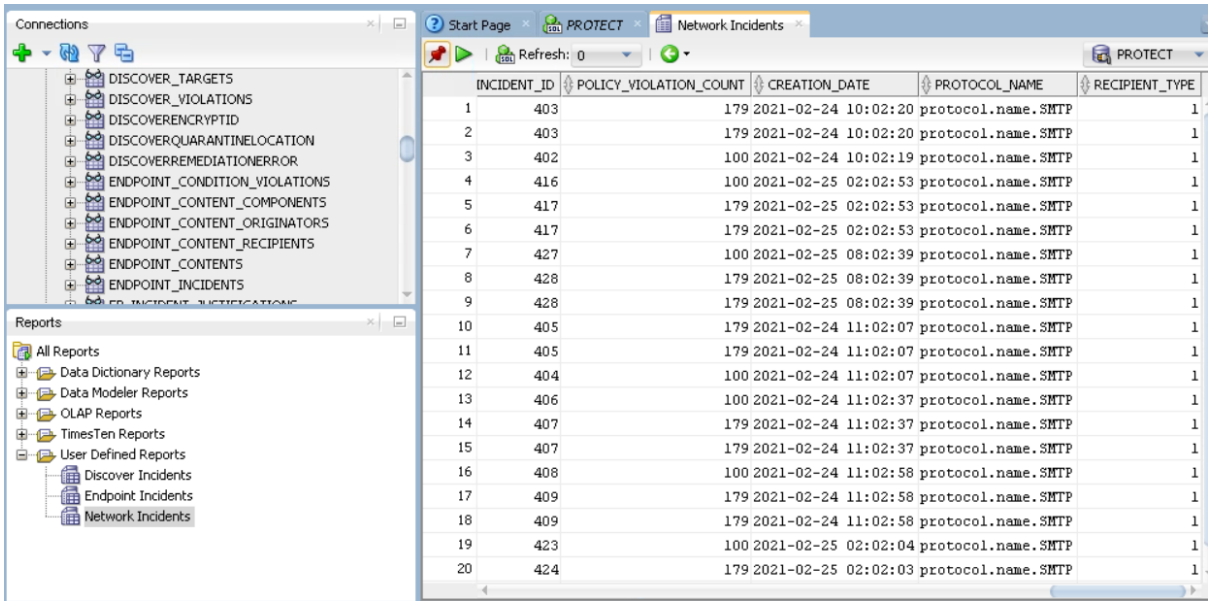
Displaying the network incidents.



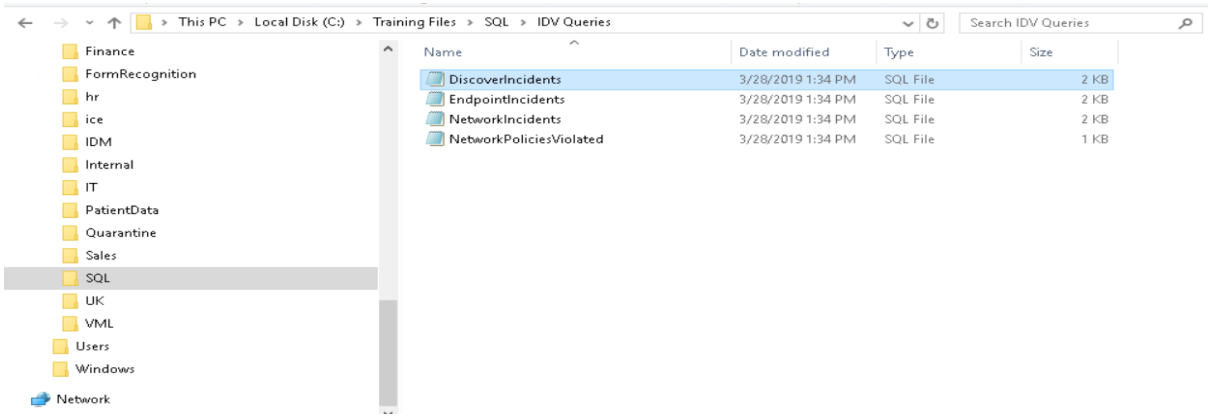
Displaying the network incidents in detail



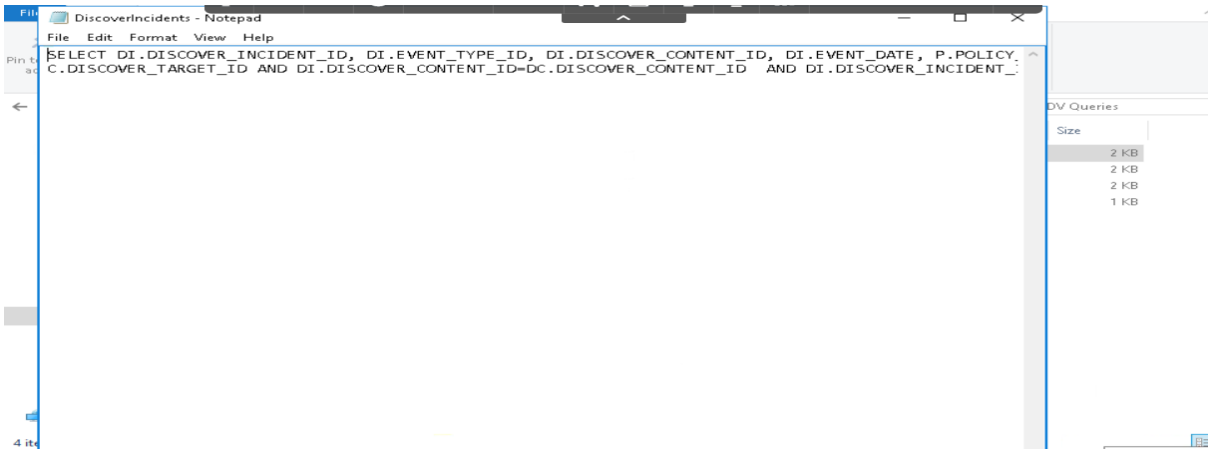
Displaying the network incidents in detail



Displaying the network incidents in detail



Sql queries in the IDV queries



Displaying the query.

Exercise 5:

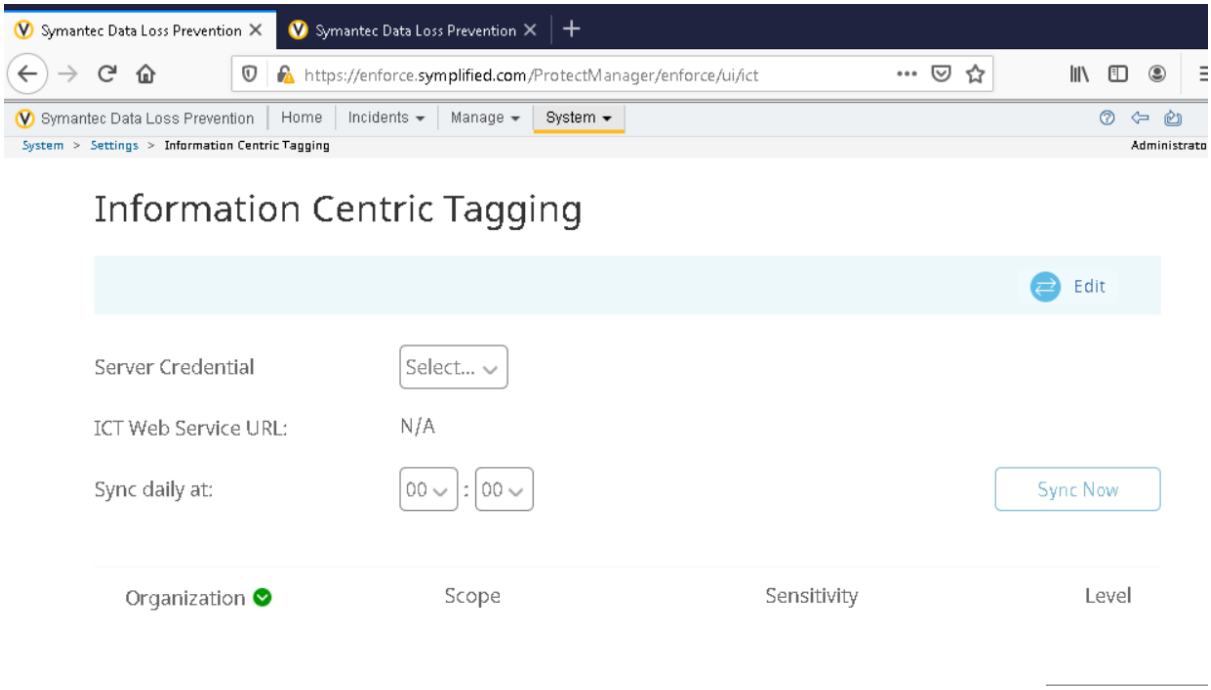
Create the ICT tag policy for File Discovery.

ICT – Information Centric Tagging.

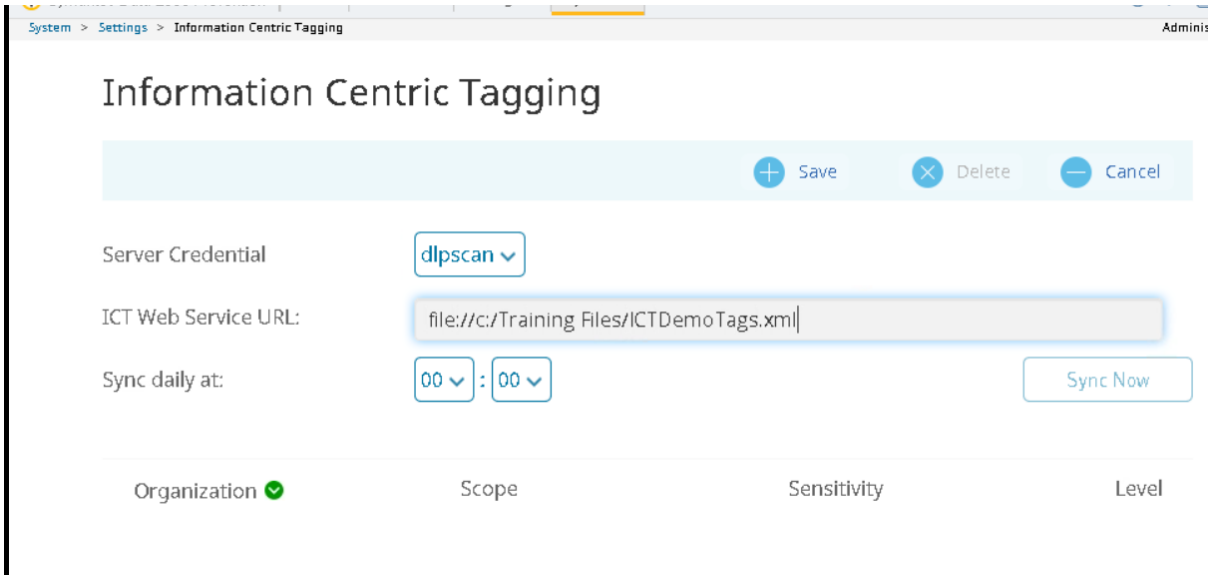
BY adding ICT it allows users to discover and identify files with certain tags as well as content identifiers.

While SYmplified doesn’t have ICT to work with files and tag taxinomoies that have already been defined and imported into this environment.

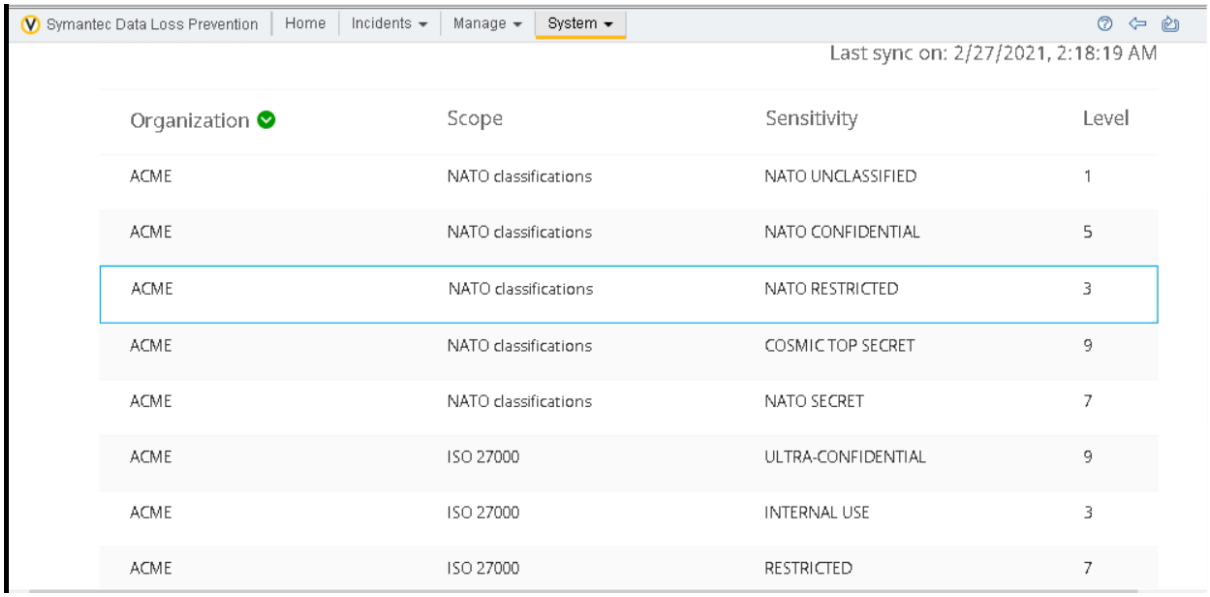
In this lab , we will link a tag taxonomy file to the enforce server so it recognizes a defined body of tags which can be used for discovery scans and policy enforecement. Then we will create a policy that looks for those tags.



Setting the new rules on clicking on the edit option

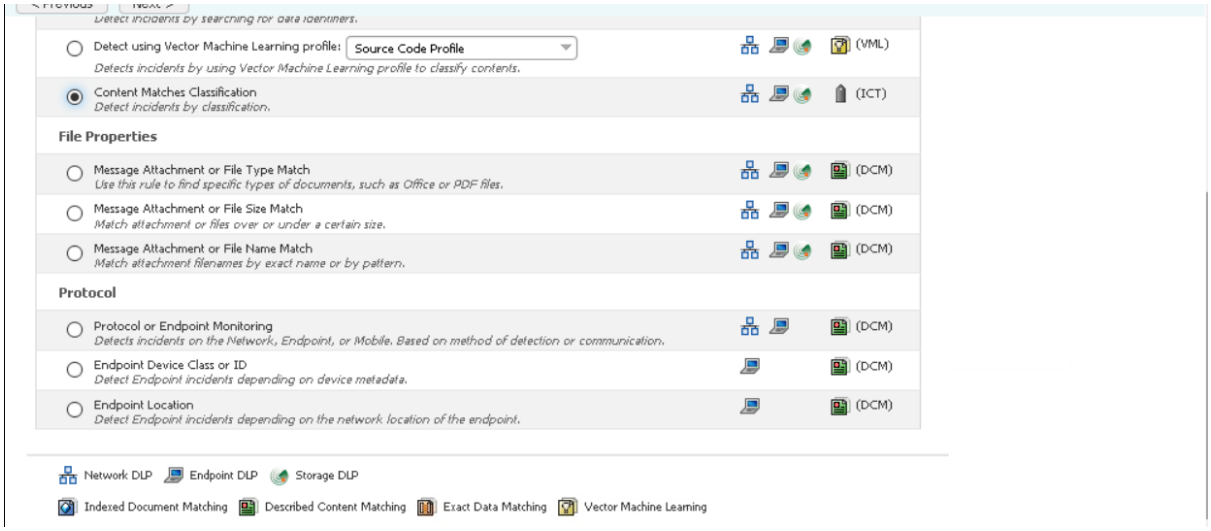


New rules In the Information Centric Tagging

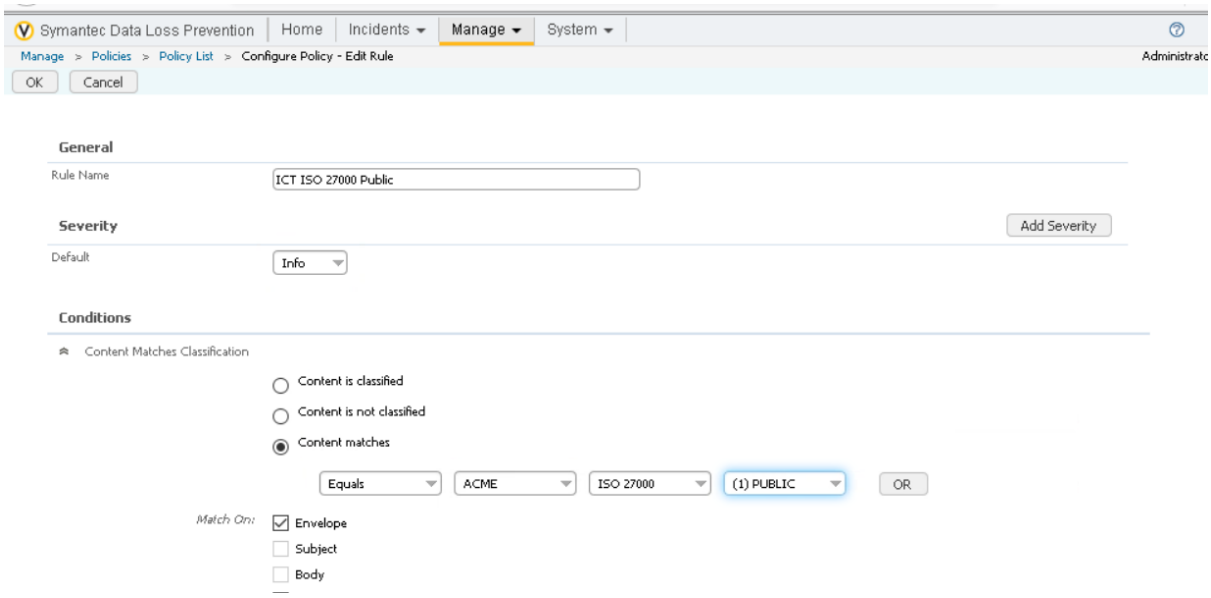


Organization	Scope	Sensitivity	Level
ACME	NATO classifications	NATO UNCLASSIFIED	1
ACME	NATO classifications	NATO CONFIDENTIAL	5
ACME	NATO classifications	NATO RESTRICTED	3
ACME	NATO classifications	COSMIC TOP SECRET	9
ACME	NATO classifications	NATO SECRET	7
ACME	ISO 27000	ULTRA-CONFIDENTIAL	9
ACME	ISO 27000	INTERNAL USE	3
ACME	ISO 27000	RESTRICTED	7

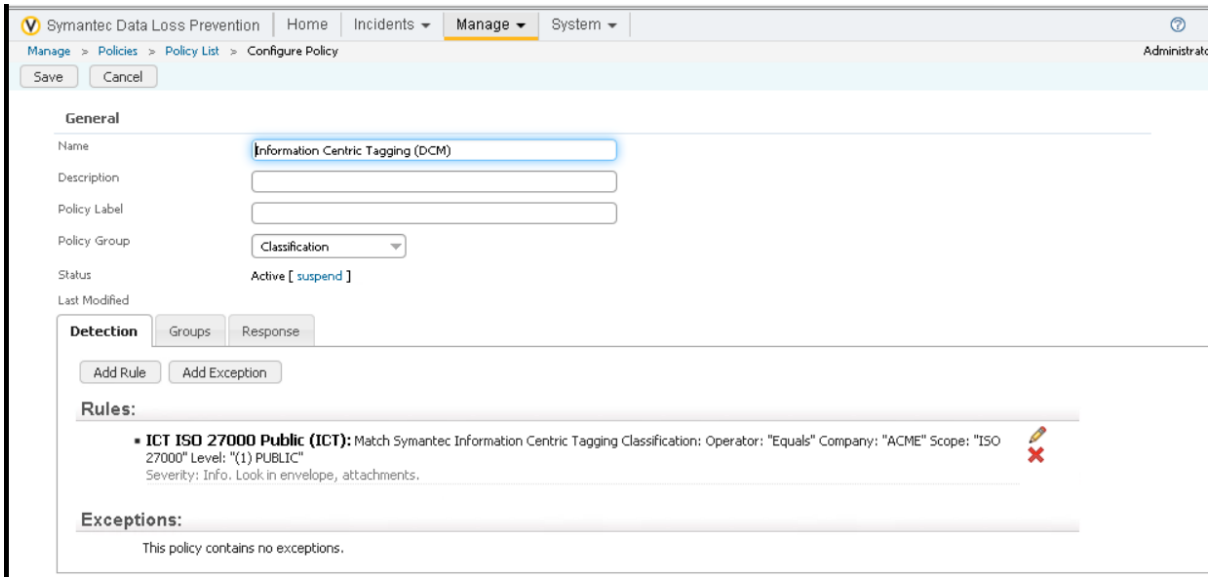
Displaying the list of new tags.



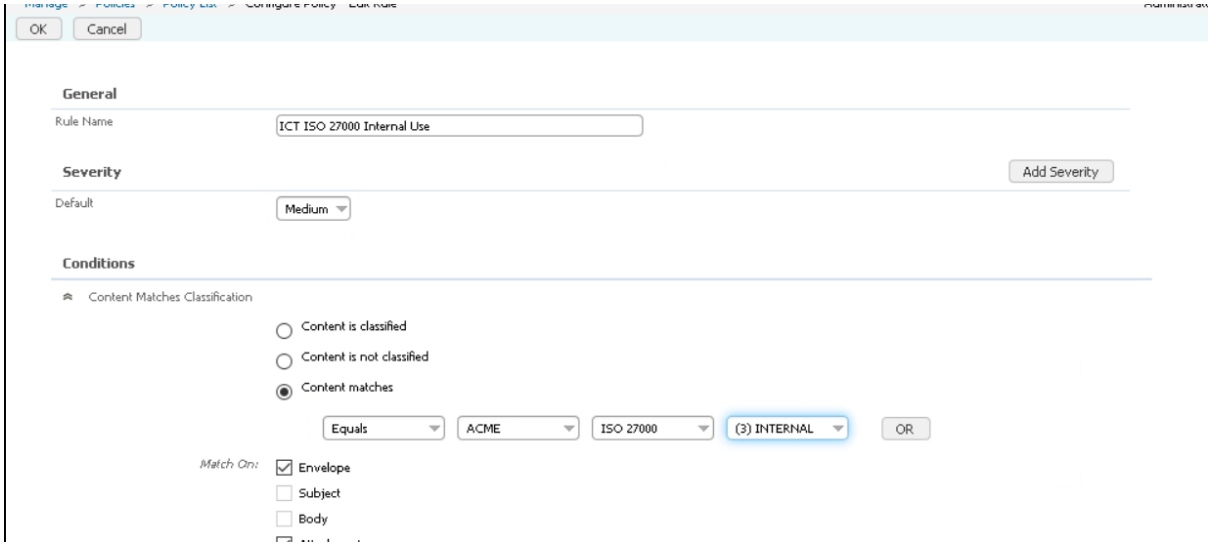
Configuring the new policy



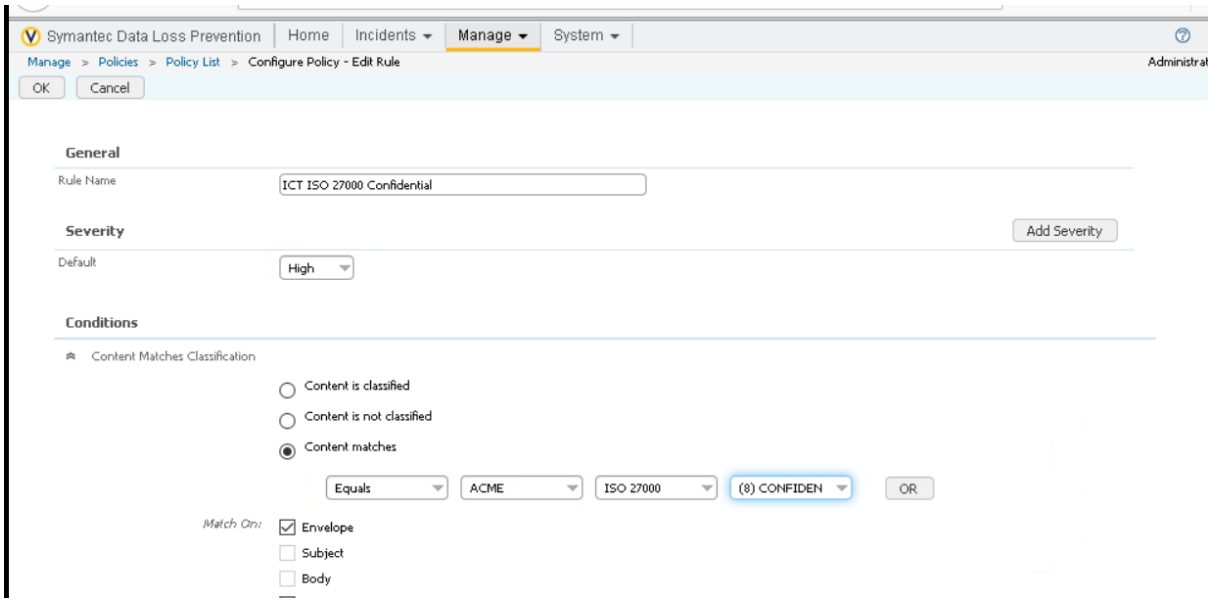
Configuring the new policy.



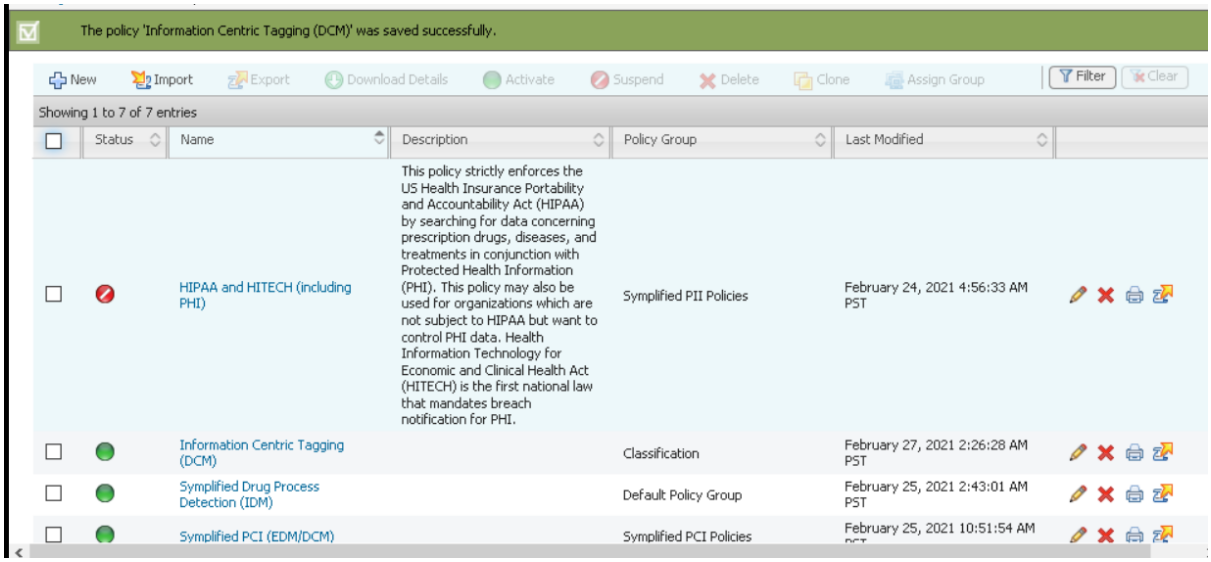
Adding the rules for the new policy



Ruled for Internal use



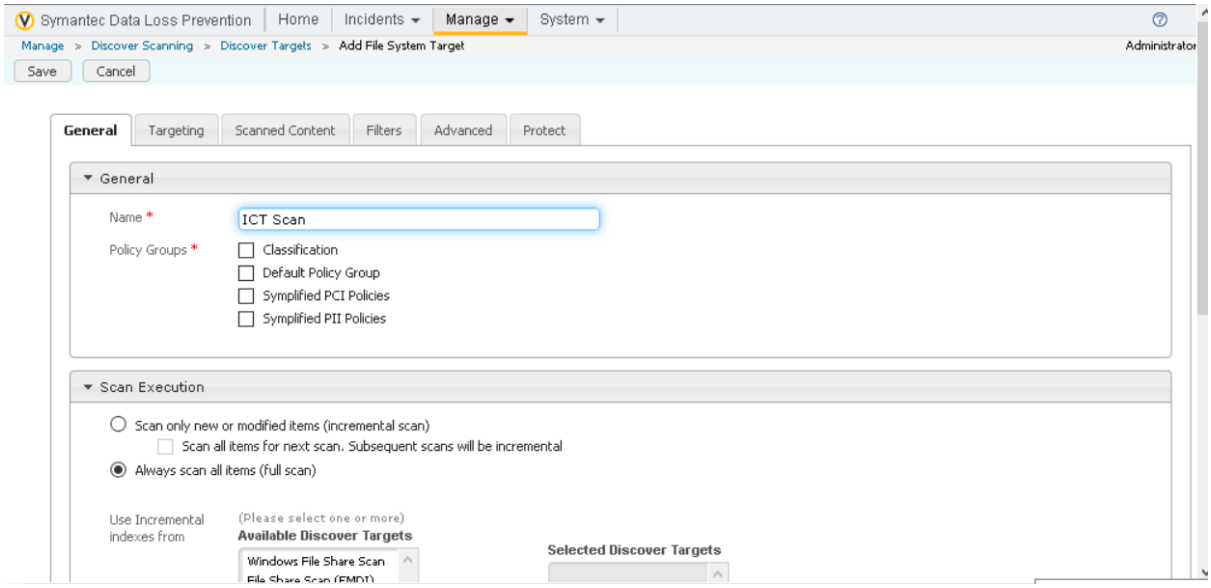
Rules for confidential



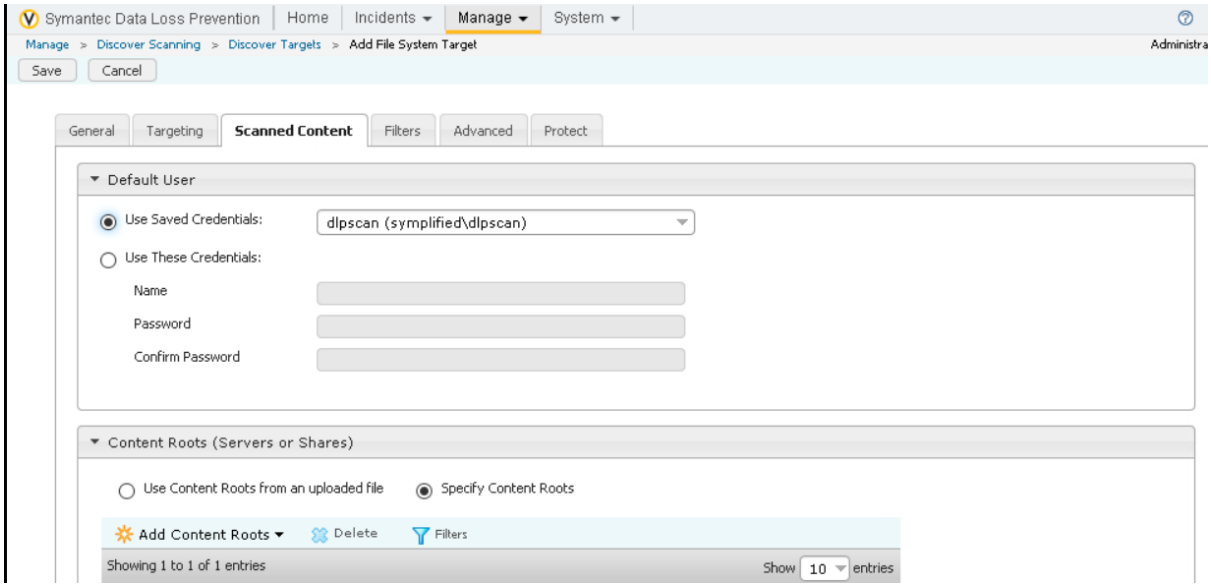
Indicates that the new policy is added

Exercise 6:

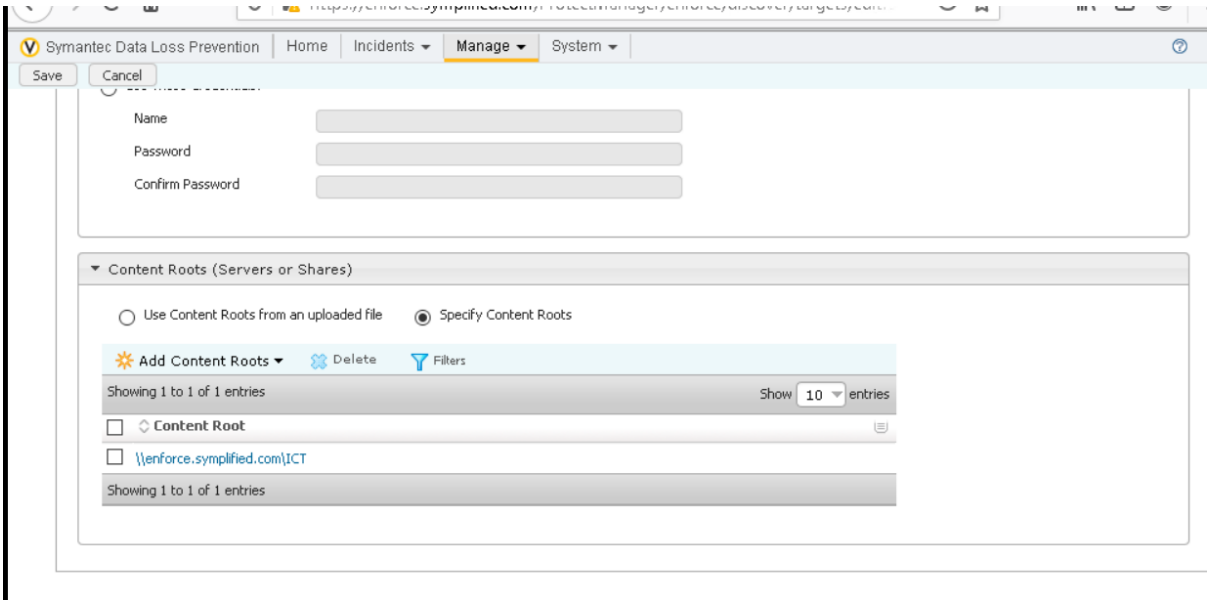
Now that the tag taxonomy and related policy has been added we can include these tag classifications in your discovery scans. In this exercise you will look for files on the endpoint computers that have been tagged with ISO-27000 tags , and will be very cautious about the files which are tagged as restricted or confidential.



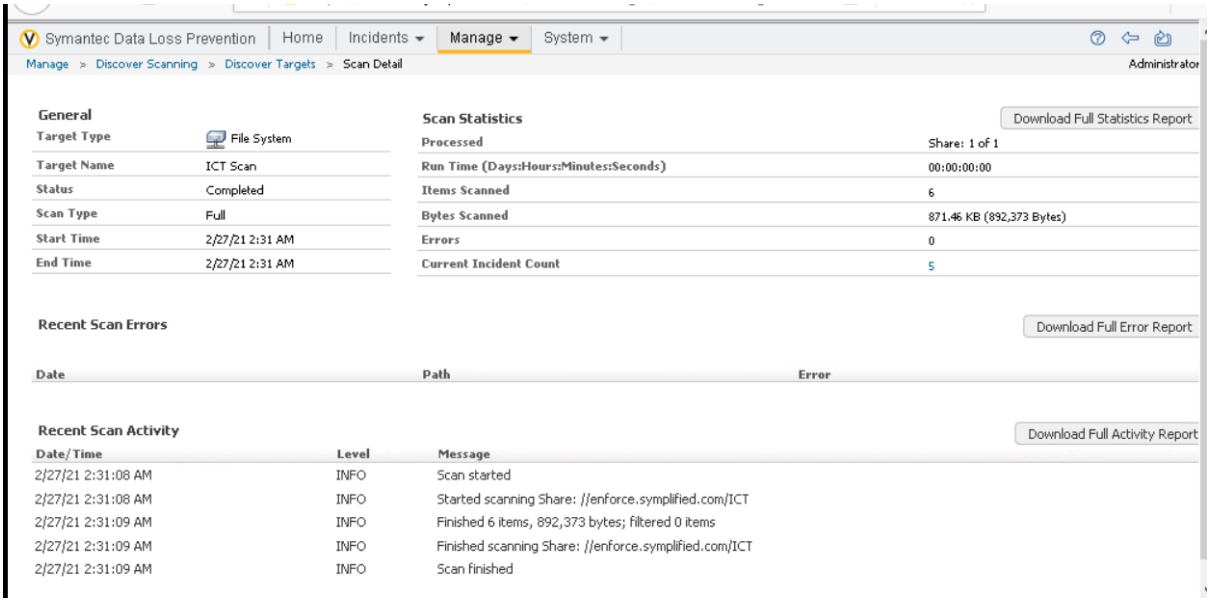
Adding the file system target



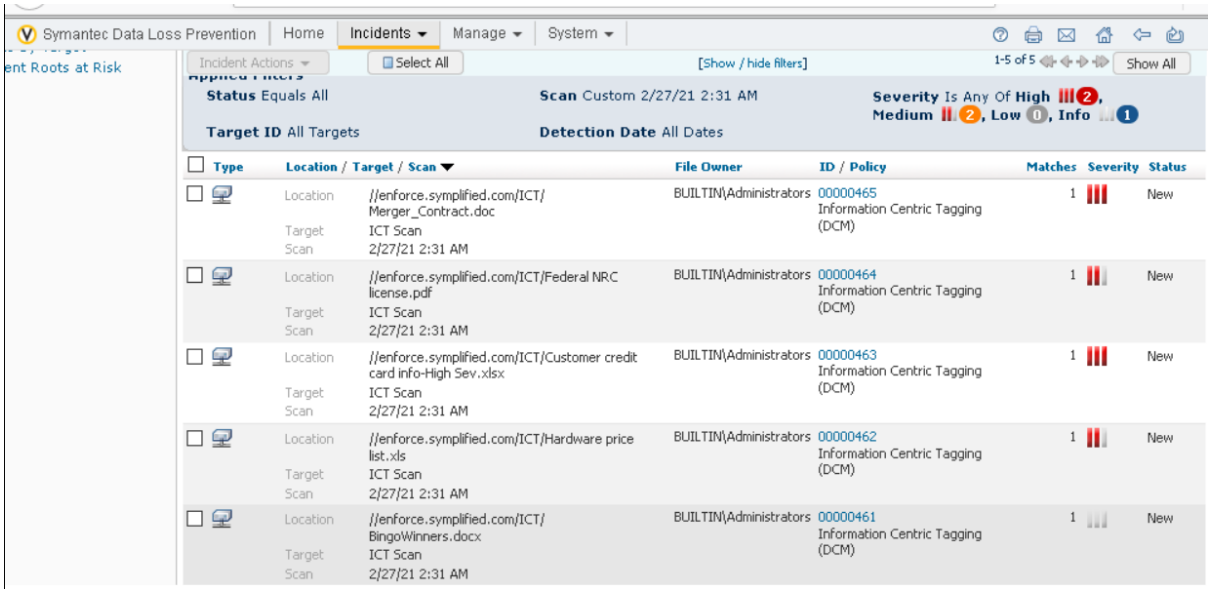
Setting the rules in Scanned Content



Rules added and need to save on this step



We can clearly see that incident count was 5.



We can clearly the 5 incidents.