ExtremeControl & DatAlert Implementation Guide

Abstract:

There are great security tools on the market. There are great network management tools on the same market. The best value for the customer is combination of both security tool and management tool. In other words the automation gives the customer great value. Varonis DatAlert automatically detect suspicious and unwatned activity across disparate platforms through analytics and in real-time, helping you spot issues and prevent data breaches. ExtremeControl solution is a multi-vendor solution that provides an unparalleled range of choices for fine-grained network access control.

Published: August 2018

Extreme Networks, Inc.
145 Rio Robles
San Jose, California 95134
Phone / +1 408.579.2800
Toll-free / +1 888.257.3000
www.extremenetworks.com

Specifications are subject to change without notice.

For information on Extreme Networks trademarks, see:

www.extremenetworks.com/company/legal/trademarks.

Contents

Use Case

DatAlert monitors enterprise assets for suspicious activity and unusual behavior, detecting critical events and compromised assets on customer core infrastructure.

Detect insider threats and cyber threats by analyzing data, account activity, and user behavior. Automate responses to suspicious activity and alert on unusual behavior – using deep analysis of metadata, machine learning, and advanced User Behavior Analytics (UBA).

ExtremeControl is part of Extreme Management Center (XMC). Management Center (formerly known as NetSight) is a single pane of glass management system that provides wired/wireless visibility and control from the data center to the mobile edge. The intelligence, automation, and integration of your management software enable the IT organization to optimize the efficiency of network operations and reduce total cost of ownership.

Management Center provides centralized visibility and granular control of enterprise network resources end to end. Management Center is distinctive for granularity that reaches beyond ports and VLANs down to individual users, applications, and protocols. No matter how many moves, adds, or changes occur in your environment, Management Center keeps everything in view and under control through role-based access controls. One click can equal a thousand actions when you manage your network with Extreme Networks. Management Center can even manage beyond Extreme Networks switching, routing, and wireless hardware to deliver standards-based control of other vendors' network equipment.

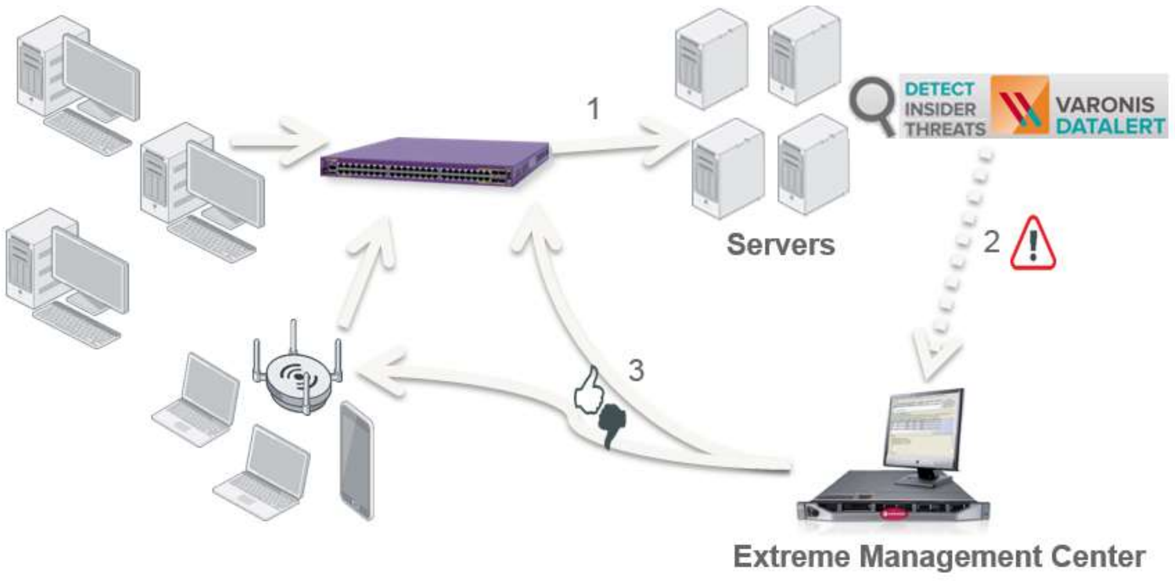
ExtremeControl is a complete standards-based, multi-vendor interoperable pre-connect and post-connect Access Control solution for wired and wireless LAN and VPN users. Using the Extreme Access Control Engine appliances and/or Virtual Appliance with XMC management configuration and reporting software, IT administrators can deploy a leading-edge Network Access Control solution to ensure only the right users have access to the right information from the right place at the right time including time of day, location, authentication types, device and OS type, and end system and user groups.

DatAlert is able to detect issues like ransomware or user suspicious activity. If such activity is detected there are several actions what can be triggered. In this integration we use custom syslog message originating from DatAlert going to XMC. The syslog message is being sent to the XMC. XMC does parse the syslog message and does decode username of the suspicious activity. Extreme Control does know what user is logged in on what endsystem and where is the endsystem connected to the network. Based on that syslog message notification all endystems where reported username is present are quarantined. The MAC address of those endsystems are assigned to the Blacklist group. Administrator can define what will happen with such endsystems. Most common approach is deny network access or limit the network access to very limited way (only DHCP and ARP). Informing the user through the captive web portal is also supported.

Example use cases = when the account can be quarantined:

- Crypto Activity Detected. There is dictionary of file names what ransomware creates in the Varonis DatAlert solution. If such file is opened, created or renamed then such account can be quarantined from the network.

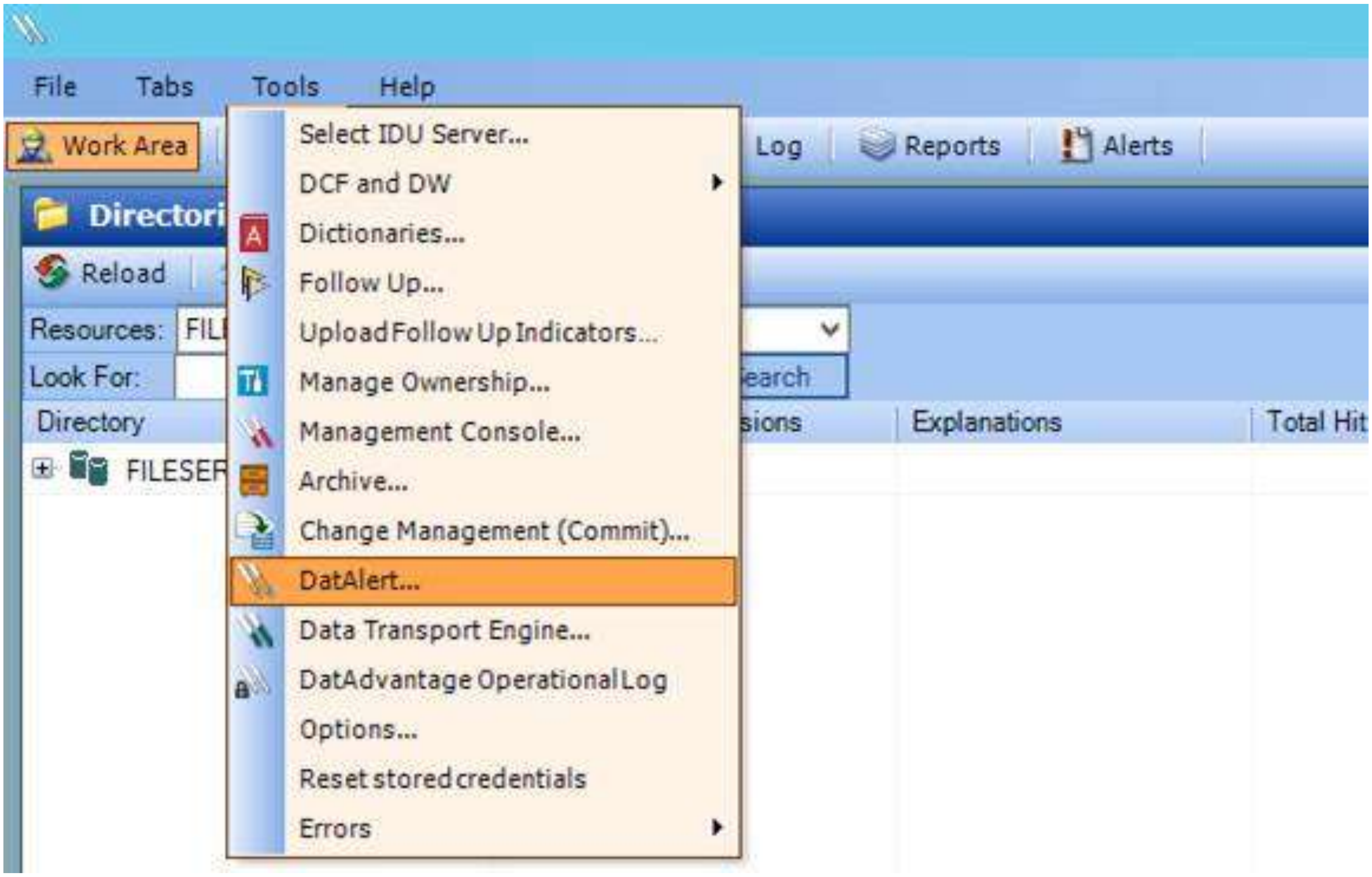
- Abnormal Behavior: Unusual Number of File Deletion. Varonis DatAlert is learning the behavior of users. If there is abnormal amount of files deleted from protected servers then the alarm is triggered. Threshold can be also configured. Such account can be quarantined from the network.
- Membership Changes: Admin Groups. If the company does out-source some services, it is very common that outsourced company does need admin access to accomplish contracted duties. If such out-sourced account with admin priviledges does add priviledges to another account it is evidence of breaking the out-sourcing contract. Such account can be quarantined from the network.
- Modification: Critical GPOs. If any of critical Group Policy Objects is modified by not authorized account the account can be quarantined from the network.



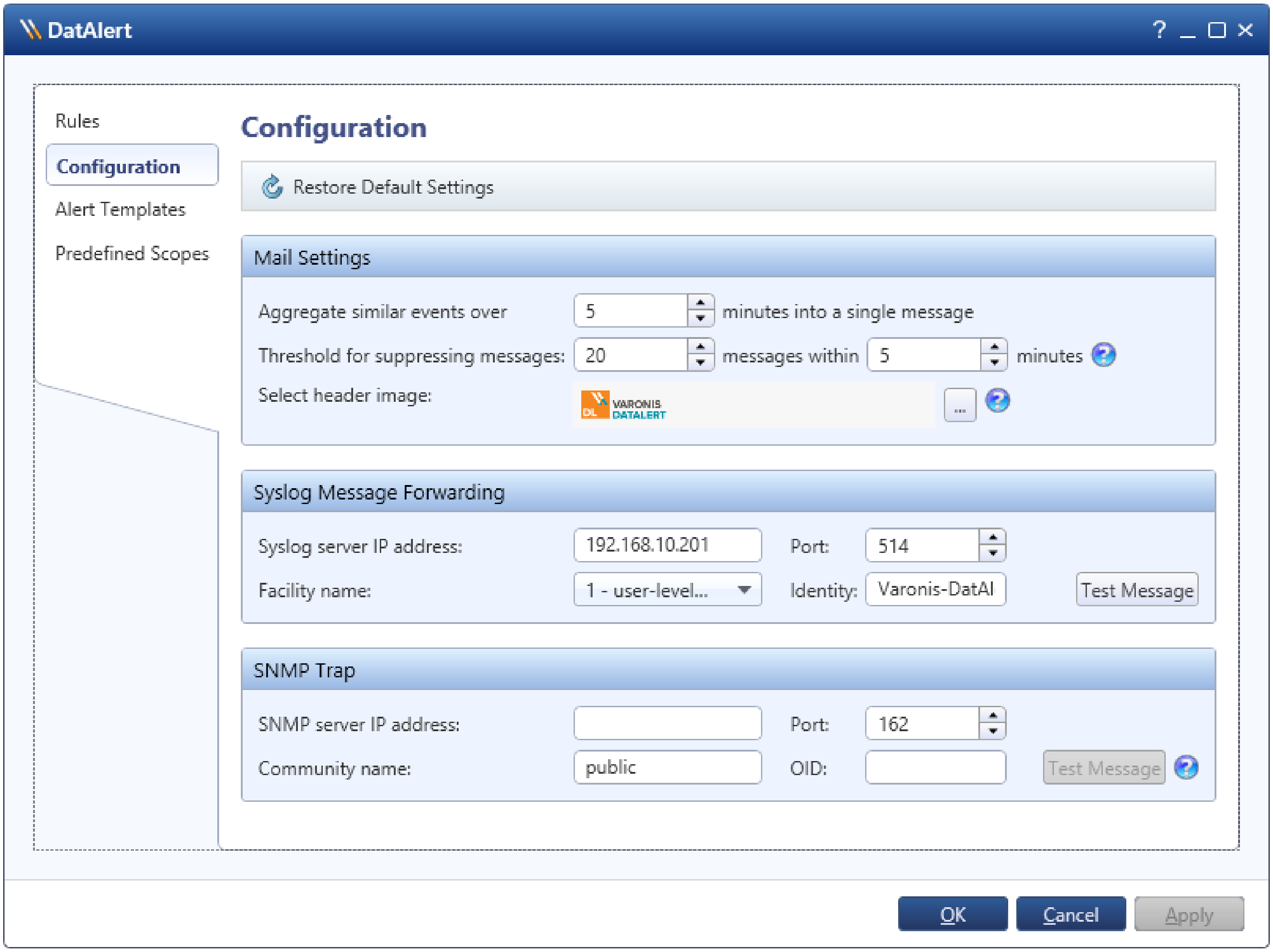
1. User behavior is analyzed by Varonis DatAlert.
2. Ransomware is detected or attack is detected by Varonis DatAlert => EMC is notified by message.
3. Extreme Management Center initiates reaction against all machines where the user is located.

Varonis DatAlert configuration

1) Run the DatAlert configuration from the DatAdvantage menu



2) SYSLOG configuration in DatAlert



Configuration

Mail Settings

Aggregate similar events over 5 minutes into a single message

Threshold for suppressing messages: 20 messages within 5 minutes

Select header image:

Syslog Message Forwarding

Syslog server IP address: 192.168.10.201

Port: 514

Facility name: 1 - user-level...

Identity: Varonis-DatAl

SNMP Trap

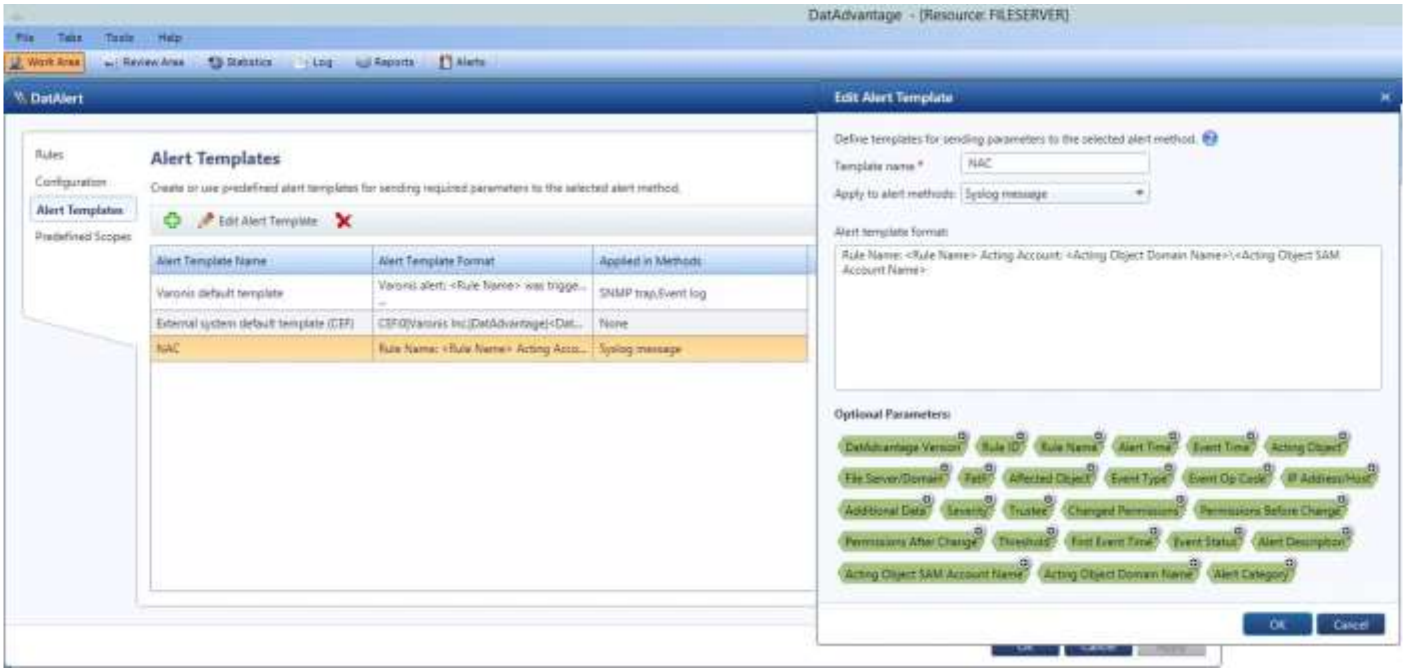
SNMP server IP address:

Port: 162

Community name: public

OID:

3) Create Alert Template for SYSLOG



Alert Templates

Create or use predefined alert templates for sending required parameters to the selected alert method.

Alert Template Name	Alert Template Format	Applied in Methods
Varonis default template	Varonis alert: <Rule Name> was trigge...	SNMP trap,Event log
External system default template (CEF)	CEF:0|Varonis Inc.|DatAdvantage|<Dat...	None
NAC	Rule Name: <Rule Name> Acting Acco...	Syslog message

Edit Alert Template

Define templates for sending parameters to the selected alert method.

Template name *: NAC

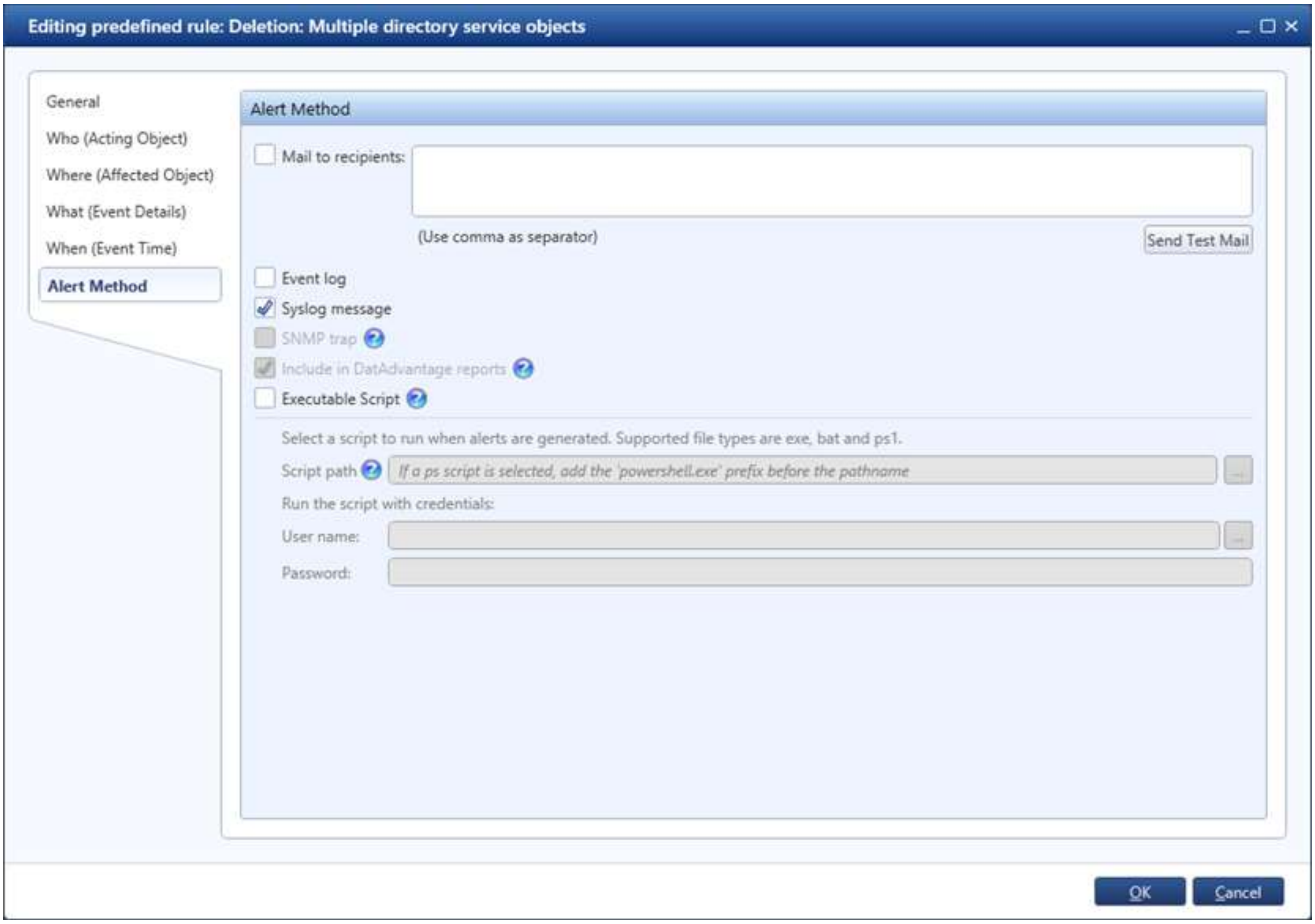
Apply to alert methods: Syslog message

Alert template format:

Rule Name: <Rule Name> Acting Account: <Acting Object Domain Name>\<Acting Object SAM Account Name>

Optional Parameters:

4) Enable SYSLOG message at the Alert method



Alert Method

□ Mail to recipients:

(Use comma as separator)

□ Event log

☑ Syslog message

□ SNMP trap

☑ Include in DatAdvantage reports

□ Executable Script

Select a script to run when alerts are generated. Supported file types are exe, bat and ps1.

Script path: *If a ps script is selected, add the 'powershell.exe' prefix before the pathname*

Run the script with credentials:

User name:

Password:

Varonis DatAlart tuning

By default the DatAlert does report the information with 60 seconds delay.

If needed you may edit file: Varonis\DatAdvantage\Probe\VrnsProbeSvc.exe.varonis.config

Find the section: <configuration><probe><filer><win> and modify:

Replace original values with new values:

Original value	New value
<add key="EnablePatternFilter" value="1"/>	<add key="EnablePatternFilter" value="0"/>
<add key="[long]QueueWaitTime" value="60000" />	<add key="[long]QueueWaitTime" value="10000" />

QueueWaitTime = how often does the sensor connect to file server and gather events. Value in miliseconds.

EnablePatternFilter = does filter temporary files which are part of short sequence of actions. Example is file deleted immediately after creation, file rename after creation.

ExtremeControl configuration

1) Upload the script to the XMC by SCP or winSCP to the /
2) ssh to the XMC
3) Create user account if the XMC is not configured to use external authentication

```
root@XMC:~$ adduser --force-badname APIuser
Allowing use of questionable username.
Adding user `APIuser' ...
Adding new group `APIuser' (1001) ...
Adding new user `APIuser' (1001) with group `APIuser' ...
Creating home directory `/home/APIuser' ...
Copying files from `/etc/skel' ...
Enter new UNIX password: password
Retype new UNIX password: password
passwd: password updated successfully
Changing the user information for APIuser
Enter the new value, or press ENTER for the default
        Full Name []:
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n] y
```

4) Unpack the script

```
root@XMC:/$ tar xfz varonis2quarantine.tgz
root@XMC:/$ chmod 750 /usr/local/bin/varonis2quarantine.sh
```

5) Update the credentials in the script and the IP

```
root@XMC:/$ cat /usr/local/bin/varonis2quarantine.sh
#!/bin/sh
ARGs=$@
APIUSERNAME=APIuser
APIPASSWORD=password
NMS=127.0.0.1
DESCRIPTION=$ARGs

/usr/bin/logger "AutoBlacklist started"
DOMAIN=`echo "$ARGs" | grep -oP 'Acting\sAccount:\s.+' | cut -d ":" -f2 |
sed "s/ //g" | cut -d '\\' -f1 | tr [a-z] [A-Z] | cut -d '.' -f1`
USER=`echo "$ARGs" | grep -oP 'Acting\sAccount:\s.+' | cut -d ":" -f2 |
sed "s/ //g" | cut -d '\\' -f2`
USERNAME="$DOMAIN\\$USER"
DESCRIPTION=`echo "$ARGs" | grep -oP 'Rule\sName:\s.+' | sed  "s/ /%20/g"`

/usr/bin/logger "AutoBlacklist searching for $USERNAME"
```

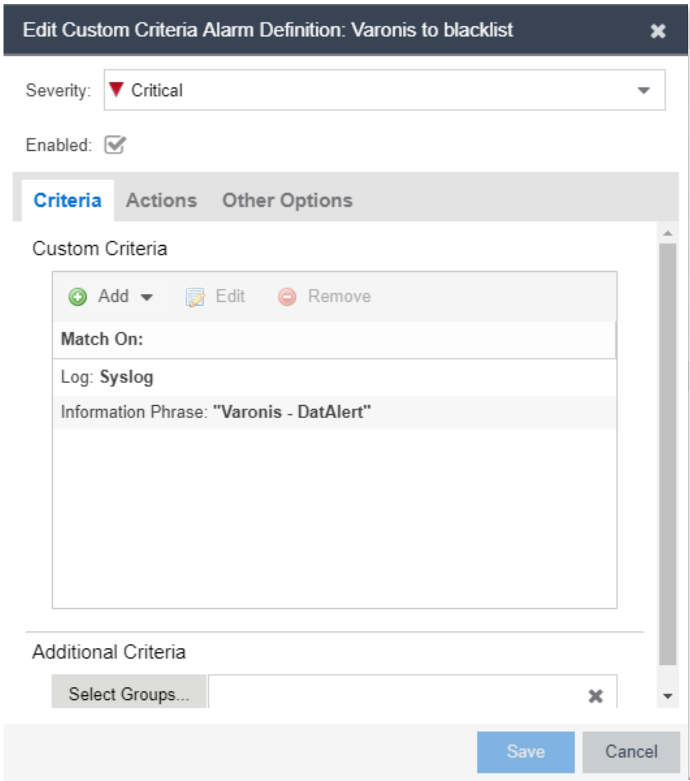
```
MACS=`/usr/bin/curl -u $APIUSERNAME:$APIPASSWORD -k  -s
"https://$NMS:8443/axis/services/NACEndSystemWebService/getEndSystemsByUse
rName?userName=$USERNAME" | sed "s/,/\n/g" | grep macAddress= | cut -d "="
-f2`

/usr/bin/logger "AutoBlacklist applying blacklist for $MACS"

j=1
for i in $MACS
do
MAC=`echo $MACS |cut -d " " -f$j`
/usr/bin/curl -u $APIUSERNAME:$APIPASSWORD -k  -s
"https://$NMS:8443/axis/services/NACWebService/addMACToBlacklist?macAddres
s=$MAC&description=$DESCRIPTION&reauthenticate=true">/dev/nul
j=`expr $j + 1`
done

/usr/bin/logger "AutoBlacklist done"
```

6) XMC Alarm configuration
If the Syslog does contain phrase „Varonis - DatAlert“ then execute the script



Edit Custom Criteria Alarm Definition: Varonis to blacklist

Severity: Critical

Enabled: ☑

Criteria | Actions | Other Options

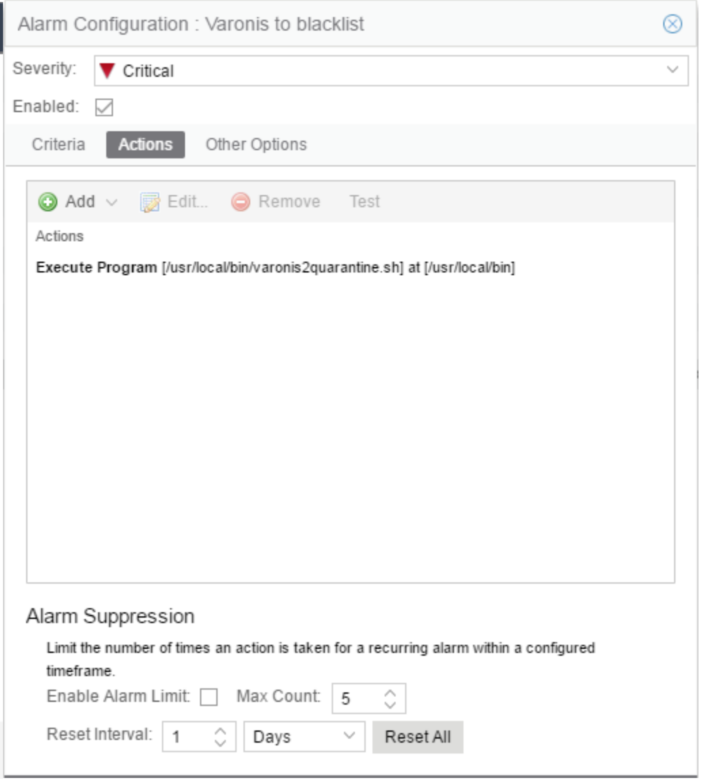
Custom Criteria

Match On:

Log: Syslog

Information Phrase: "Varonis - DatAlert"

Additional Criteria



Alarm Configuration : Varonis to blacklist

Severity: Critical

Enabled: ☑

Criteria | Actions | Other Options

Actions

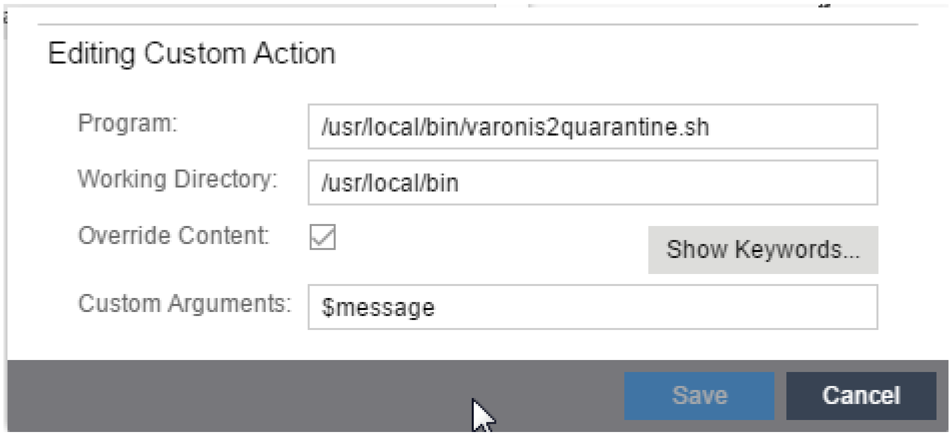
Execute Program [/usr/local/bin/varonis2quarantine.sh] at [/usr/local/bin]

Alarm Suppression

Limit the number of times an action is taken for a recurring alarm within a configured timeframe.

Enable Alarm Limit: □ Max Count: 5

Reset Interval: 1 Days



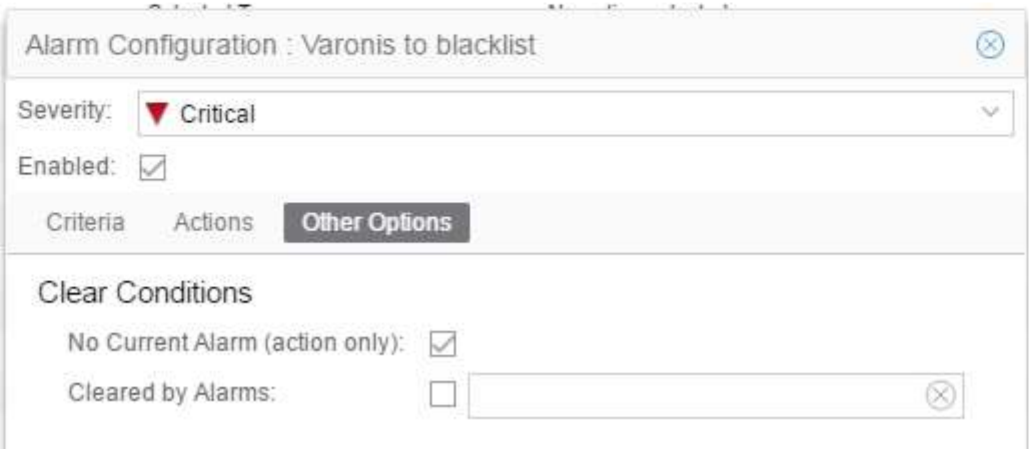
Editing Custom Action

Program: /usr/local/bin/varonis2quarantine.sh

Working Directory: /usr/local/bin

Override Content: ☑

Custom Arguments: $message



Alarm Configuration : Varonis to blacklist

Severity: Critical

Enabled: ☑

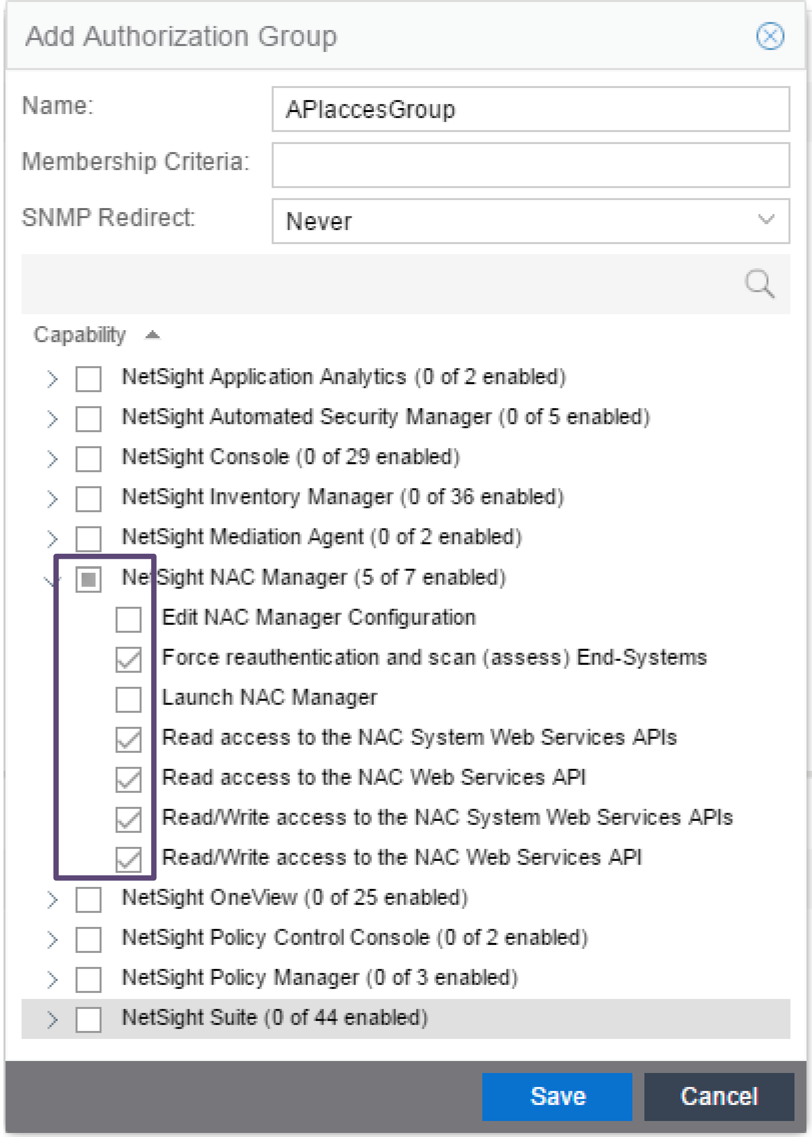
Criteria | Actions | Other Options

Clear Conditions

No Current Alarm (action only): ☑

Cleared by Alarms: □

7) API access configuration
Create Authorization Group with following capability:



Add Authorization Group

Name: APIaccesGroup

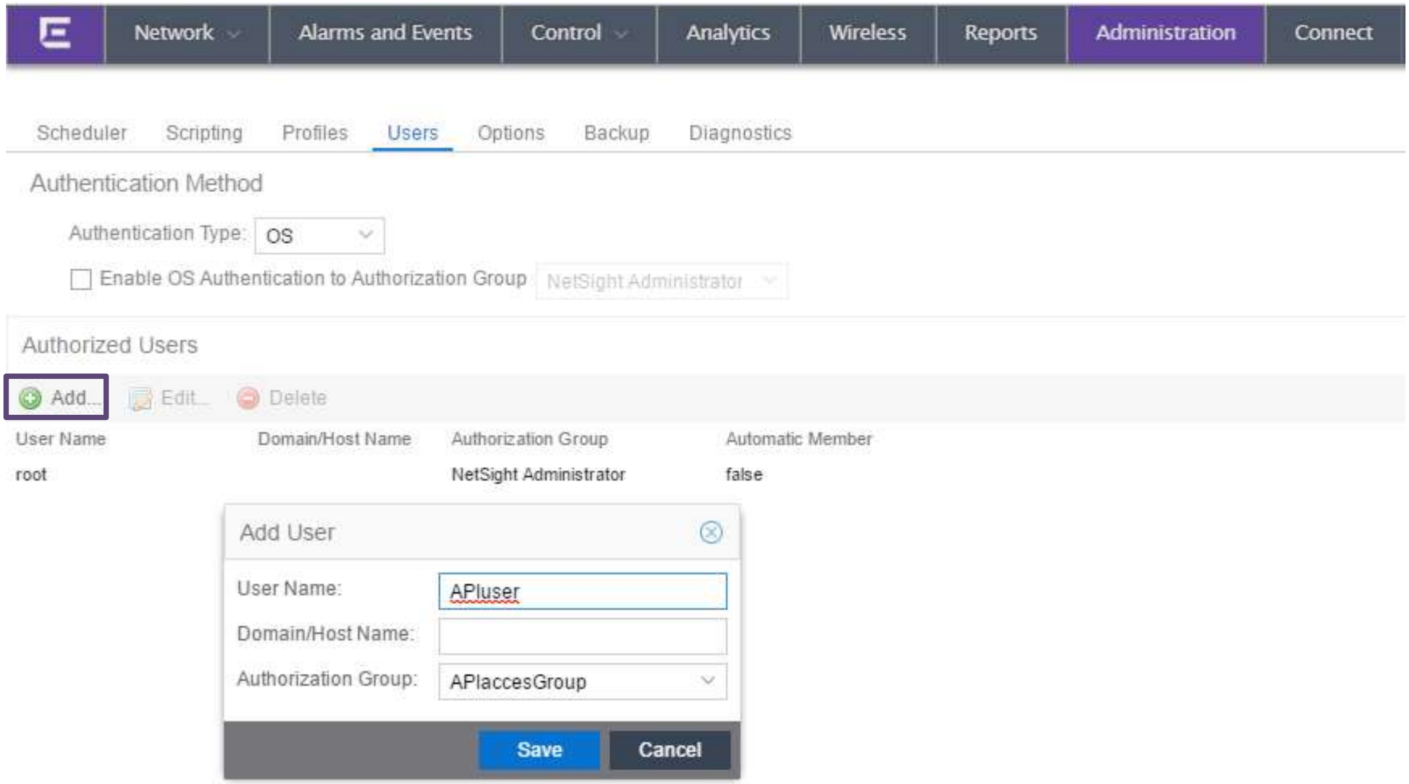
Membership Criteria:

SNMP Redirect: Never

Capability

- □ NetSight Application Analytics (0 of 2 enabled)
- □ NetSight Automated Security Manager (0 of 5 enabled)
- □ NetSight Console (0 of 29 enabled)
- □ NetSight Inventory Manager (0 of 36 enabled)
- □ NetSight Mediation Agent (0 of 2 enabled)
- ■ NetSight NAC Manager (5 of 7 enabled)
  - □ Edit NAC Manager Configuration
  - ☑ Force reauthentication and scan (assess) End-Systems
  - □ Launch NAC Manager
  - ☑ Read access to the NAC System Web Services APIs
  - ☑ Read access to the NAC Web Services API
  - ☑ Read/Write access to the NAC System Web Services APIs
  - ☑ Read/Write access to the NAC Web Services API
- □ NetSight OneView (0 of 25 enabled)
- □ NetSight Policy Control Console (0 of 2 enabled)
- □ NetSight Policy Manager (0 of 3 enabled)
- □ NetSight Suite (0 of 44 enabled)

8) API access configuration
Add APIuser to the authorization group



Authentication Method

Authentication Type: OS

□ Enable OS Authentication to Authorization Group NetSight Administrator

Authorized Users

User Name	Domain/Host Name	Authorization Group	Automatic Member
root		NetSight Administrator	false

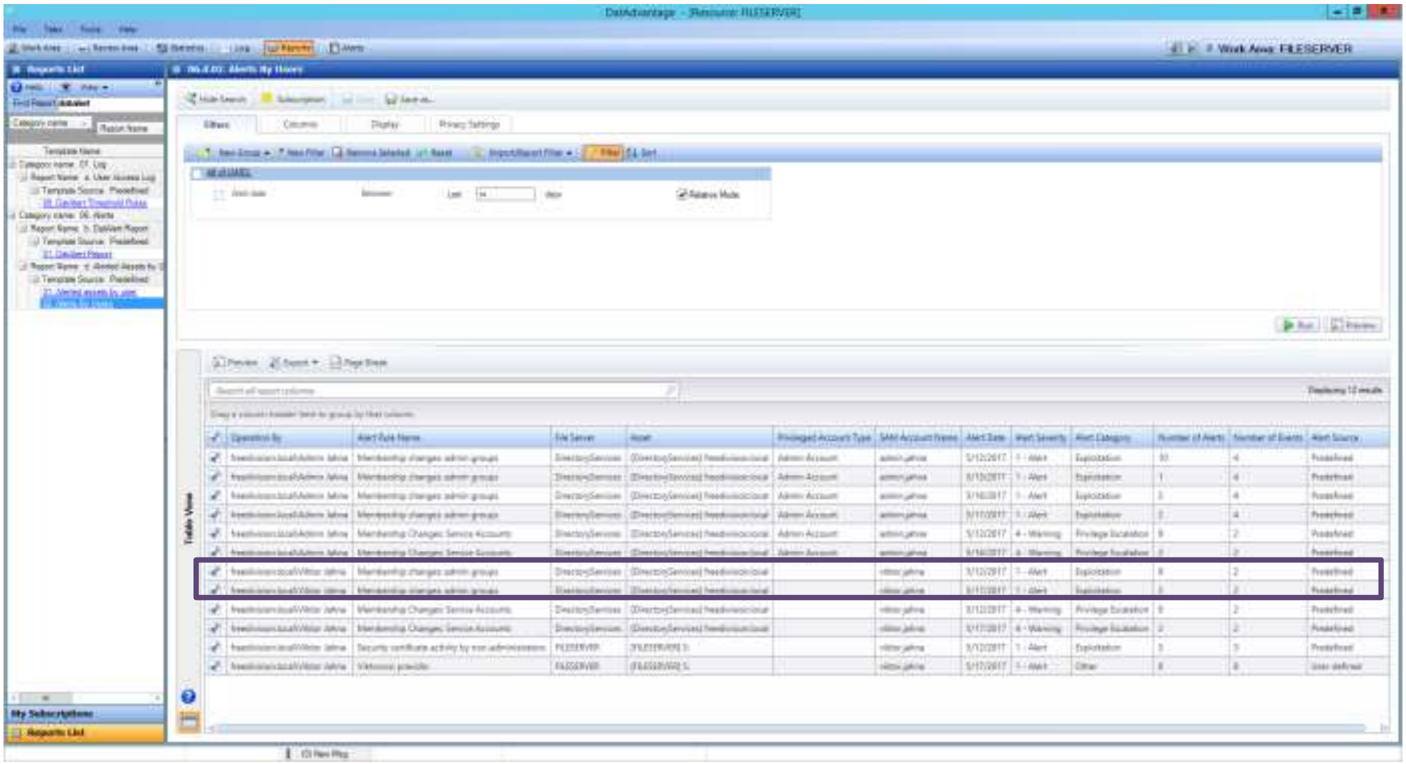
Add User

User Name: APIuser

Domain/Host Name:

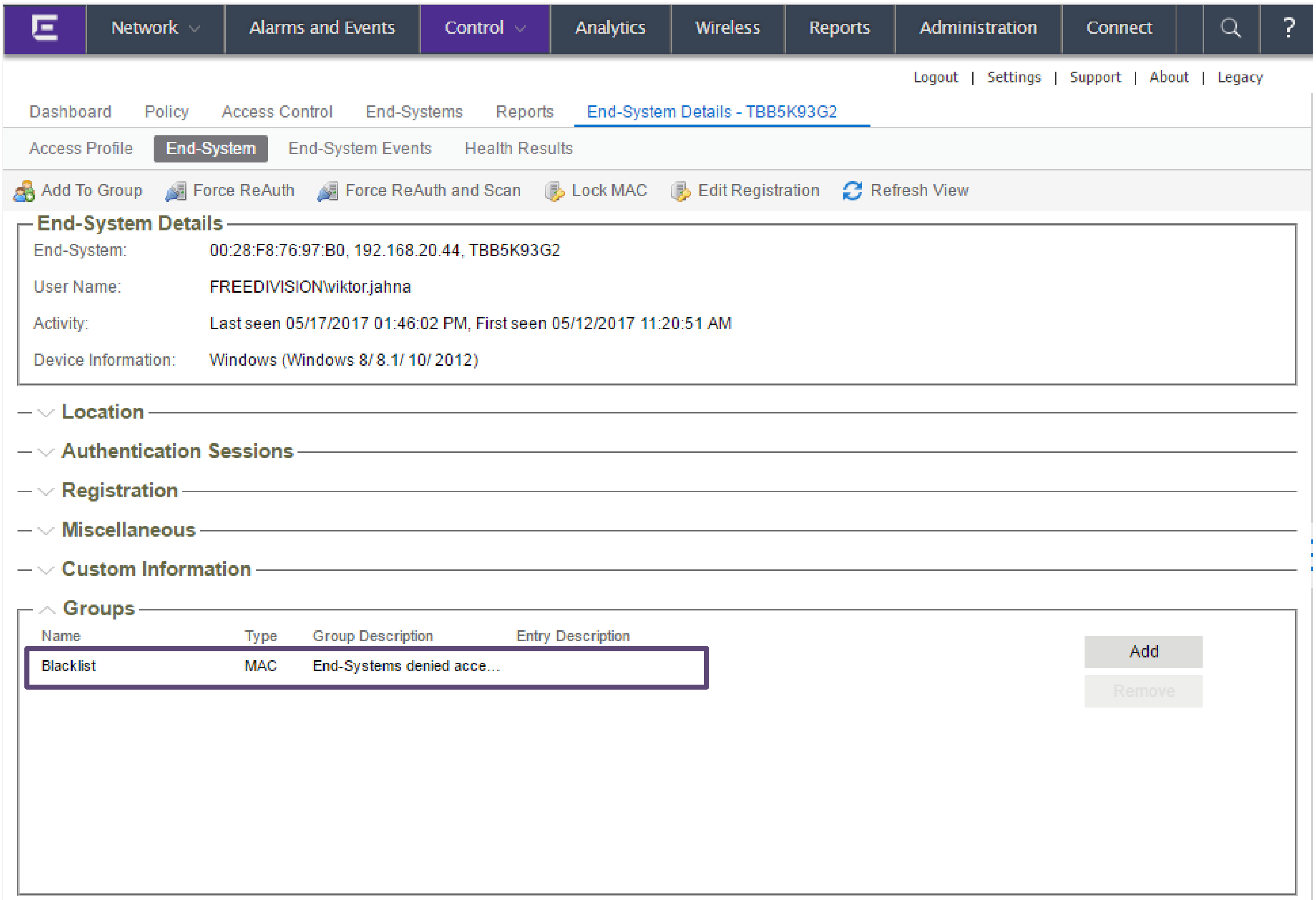
Authorization Group: APIaccesGroup

Verification it works



Displaying 12 results

✓	Operation By	Alert Rule Name	File Server	Asset	Privileged Account Type	SAM Account Name	Alert Date	Alert Severity	Alert Category	Number of Alerts	Number of Events	Alert Source
✓	freedivision.local\Admin Jahna	Membership changes admin groups	DirectoryServices	[DirectoryServices] freedivision.local	Admin Account	admin.jahna	5/12/2017	1 - Alert	Exploitation	10	4	Predefined
✓	freedivision.local\Admin Jahna	Membership changes admin groups	DirectoryServices	[DirectoryServices] freedivision.local	Admin Account	admin.jahna	5/15/2017	1 - Alert	Exploitation	1	4	Predefined
✓	freedivision.local\Admin Jahna	Membership changes admin groups	DirectoryServices	[DirectoryServices] freedivision.local	Admin Account	admin.jahna	5/16/2017	1 - Alert	Exploitation	3	4	Predefined
✓	freedivision.local\Admin Jahna	Membership changes admin groups	DirectoryServices	[DirectoryServices] freedivision.local	Admin Account	admin.jahna	5/17/2017	1 - Alert	Exploitation	2	4	Predefined
✓	freedivision.local\Admin Jahna	Membership Changes Service Accounts	DirectoryServices	[DirectoryServices] freedivision.local	Admin Account	admin.jahna	5/12/2017	4 - Warning	Privilege Escalation	8	2	Predefined
✓	freedivision.local\Admin Jahna	Membership Changes Service Accounts	DirectoryServices	[DirectoryServices] freedivision.local	Admin Account	admin.jahna	5/16/2017	4 - Warning	Privilege Escalation	3	2	Predefined
✓	freedivision.local\Viktor Jahna	Membership changes admin groups	DirectoryServices	[DirectoryServices] freedivision.local		viktor.jahna	5/12/2017	1 - Alert	Exploitation	8	2	Predefined
✓	freedivision.local\Viktor Jahna	Membership changes admin groups	DirectoryServices	[DirectoryServices] freedivision.local		viktor.jahna	5/17/2017	1 - Alert	Exploitation	3	2	Predefined
✓	freedivision.local\Viktor Jahna	Membership Changes Service Accounts	DirectoryServices	[DirectoryServices] freedivision.local		viktor.jahna	5/12/2017	4 - Warning	Privilege Escalation	8	2	Predefined
✓	freedivision.local\Viktor Jahna	Membership Changes Service Accounts	DirectoryServices	[DirectoryServices] freedivision.local		viktor.jahna	5/17/2017	4 - Warning	Privilege Escalation	2	2	Predefined
✓	freedivision.local\Viktor Jahna	Security certificate activity by non administrators	FILESERVER	[FILESERVER] 1:		viktor.jahna	5/12/2017	1 - Alert	Exploitation	3	3	Predefined
✓	freedivision.local\Viktor Jahna	Viktorovic pravidlo	FILESERVER	[FILESERVER] 1:		viktor.jahna	5/17/2017	1 - Alert	Other	8	8	User defined



End-System Details

End-System: 00:28:F8:76:97:B0, 192.168.20.44, TBB5K93G2

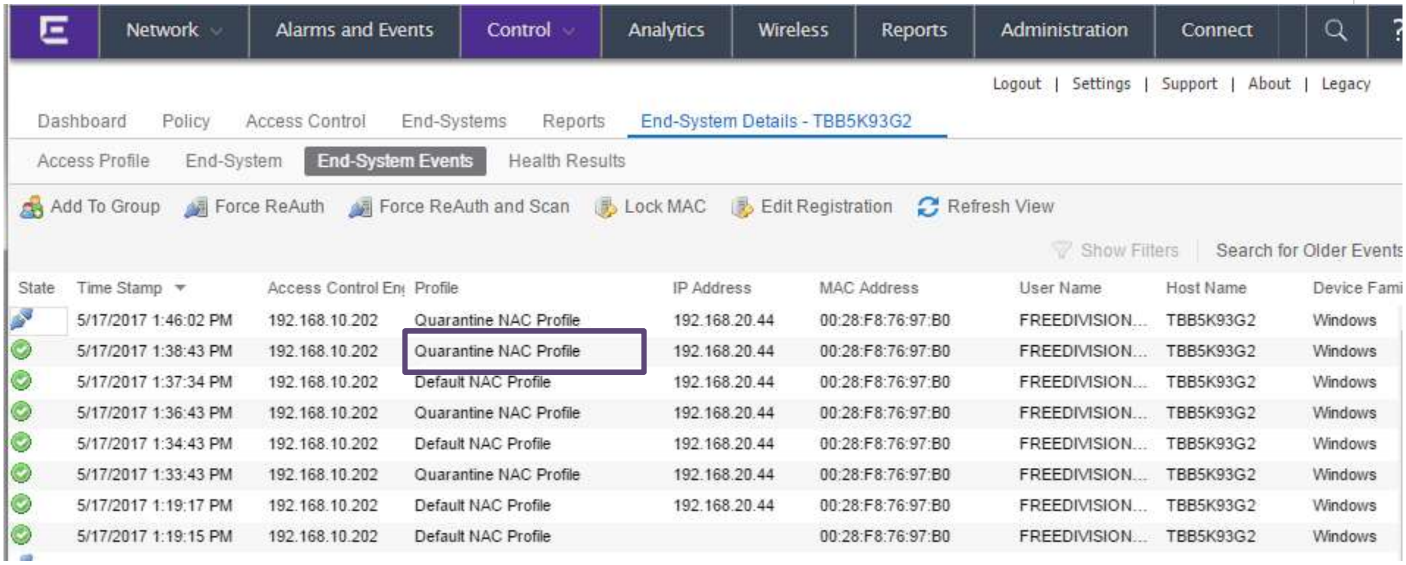
User Name: FREEDIVISION\wiktor.jahna

Activity: Last seen 05/17/2017 01:46:02 PM, First seen 05/12/2017 11:20:51 AM

Device Information: Windows (Windows 8/ 8.1/ 10/ 2012)

Groups

Name	Type	Group Description	Entry Description
Blacklist	MAC	End-Systems denied acce...	



State	Time Stamp	Access Control En(	Profile	IP Address	MAC Address	User Name	Host Name	Device Fami
	5/17/2017 1:46:02 PM	192.168.10.202	Quarantine NAC Profile	192.168.20.44	00:28:F8:76:97:B0	FREEDIVISION...	TBB5K93G2	Windows
✓	5/17/2017 1:38:43 PM	192.168.10.202	Quarantine NAC Profile	192.168.20.44	00:28:F8:76:97:B0	FREEDIVISION...	TBB5K93G2	Windows
✓	5/17/2017 1:37:34 PM	192.168.10.202	Default NAC Profile	192.168.20.44	00:28:F8:76:97:B0	FREEDIVISION...	TBB5K93G2	Windows
✓	5/17/2017 1:36:43 PM	192.168.10.202	Quarantine NAC Profile	192.168.20.44	00:28:F8:76:97:B0	FREEDIVISION...	TBB5K93G2	Windows
✓	5/17/2017 1:34:43 PM	192.168.10.202	Default NAC Profile	192.168.20.44	00:28:F8:76:97:B0	FREEDIVISION...	TBB5K93G2	Windows
✓	5/17/2017 1:33:43 PM	192.168.10.202	Quarantine NAC Profile	192.168.20.44	00:28:F8:76:97:B0	FREEDIVISION...	TBB5K93G2	Windows
✓	5/17/2017 1:19:17 PM	192.168.10.202	Default NAC Profile	192.168.20.44	00:28:F8:76:97:B0	FREEDIVISION...	TBB5K93G2	Windows
✓	5/17/2017 1:19:15 PM	192.168.10.202	Default NAC Profile		00:28:F8:76:97:B0	FREEDIVISION...	TBB5K93G2	Windows

Resources

Varonis2quarantine.tgz

Software versions

Extreme Management Center (including Extreme Control and Extreme Connect)

Tested version 8.1.35. Potential minimum version 8.0

Varonis DatAlaret

Tested version 6.3.257.58. Potential minimum version 6.0.113.12

Revision History

Table 1. Extreme Netowrks ExtremeControl & Varonis DatAlert Implementation Guide - revision history

Date	Version #	Changes Made	Author
09/06/17	0.9	Initial version	Zdeněk Pala
12/06/17	0.9.1	Fixed the picture, added some highlights	Zdeněk Pala
27/08/18	1.0	Updated screenshot, use cases, Added software version, added DatAlert tuning	Zdeněk Pala