WATSSA

West Australian Technical Support in Schools Association

INSTALLING FASTVUE

Simple Internet Usage Reporting for Fortinet Fortigate (fastvue.co)

Table of Contents

4. Version Control:

Version #		Edit By	Comments
1		Michael Raymond	First draft for setting up Fastvue Reporter
1.2		Michael Raymond	Added LDAP/Email/Securing

Metadata:

Created On: 27/04/2021 1:13:00 PM

Updated On: 13/09/2021 3:51 PM

Last Edit By: RAYMOND Michael [Duncraig Senior High School]

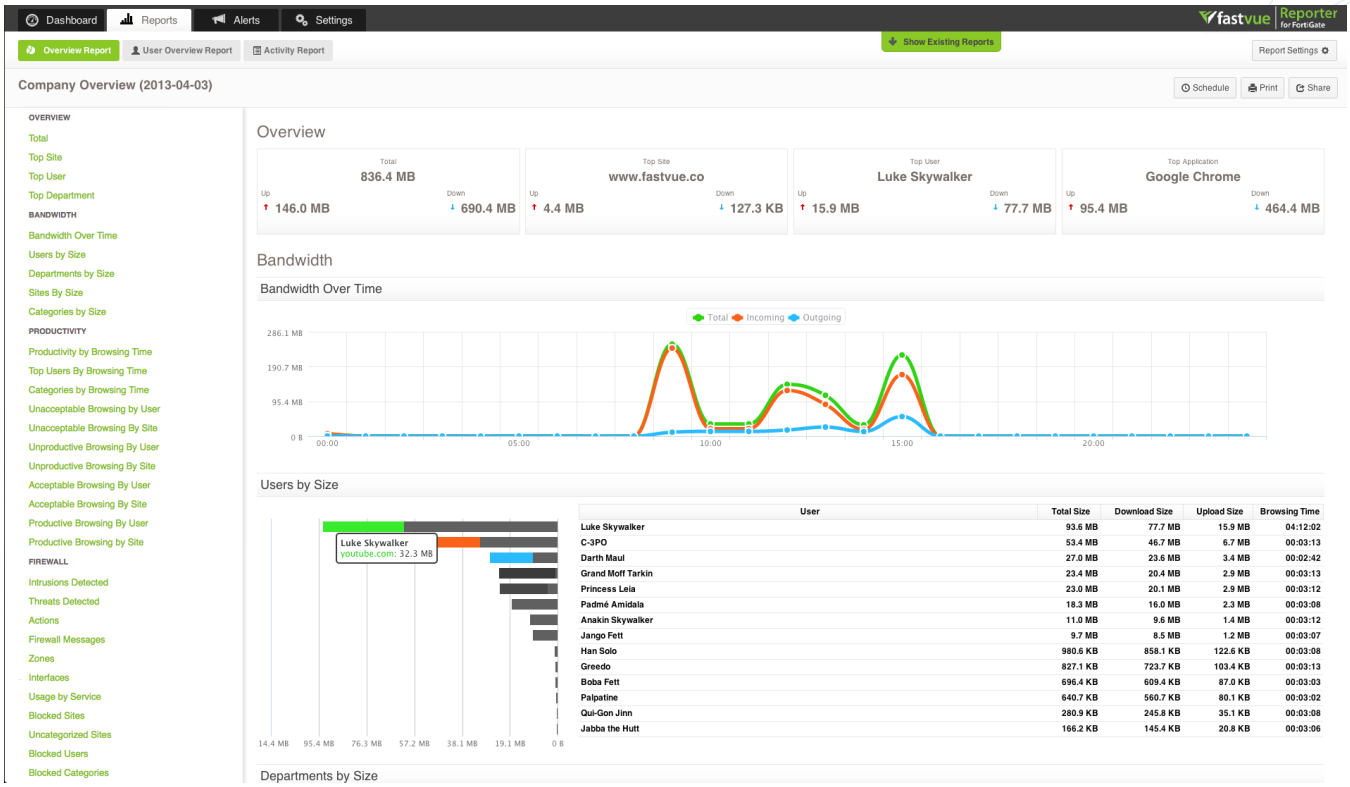
Introduction:

Fortigate Reporting Simplified!

You don't need to be a log analysis expert to understand Fastvue Reports. Designed for HR, Teachers, Department Managers and IT.

For Education

Safeguard students by monitoring access to self-harm, extremist, or inappropriate content.



1. Download and Install

Download Fastvue Reporter for FortiGate and **install** on a machine (or virtual machine) that meets our recommended requirements for your network size.

Note: *Fastvue Reporter is a resource intensive application by design in order to import data and run reports as fast as possible. We do not recommend installing Fastvue Reporter on a server that provides a critical network service such as a Domain Controller, DNS server, or DFS server. We recommend installing on a dedicated VM (virtual machine) so you can scale the resources appropriately.*

Supported Operating Systems

Fastvue Reporter is designed for **64 bit Windows Server Operating Systems** running **Windows Server 2012 R2, or above.**

Network Size Recommended Server Specification

Below 500 Users	**4 CPUs/Cores, 6 GB RAM**
500 – 1000 Users	**4 CPUs/Cores, 8 GB RAM**
1000 – 3000 Users	**8 CPUs/Cores, 12 GB RAM**
3000 – 5000 Users	**8 CPUs/Cores, 16 GB RAM**

The Fastvue Reporter installer will automatically install and configure the required pre-requisites which include .Net 4.6 and IIS (Web Server and Application Server roles). It will also install Open JDK and Elastic search in its own self-managed directory.

When installing, you will be asked to select a website to install too. If you are installing on a server with existing websites, we recommend creating a new website in IIS and installing to that. You can also choose to install to a sub-folder of an existing website (such as Default Web Site\Fastvue).

To install Fastvue Reporter:

1. Double-click the downloaded setup exe on a machine that meets the above recommendations
2. Proceed through the installation wizard to install the software. The installation wizard will ask you for:
    - **Installation folder** (defaults to C:\Program Files\Fastvue\Reporter for FortiGate). Only application files are installed to this folder. It does not require much disk space.
    - **Website and Virtual Directory** (defaults to 'Default Web Site'). If you have other websites installed on your server, it is a good idea to install Fastvue Reporter to a virtual directory such as 'fastvue' or 'fortigatereports'. Then you can access the site

at http://yourserver/fastvue for example and it does not interfere with any other site on your server.

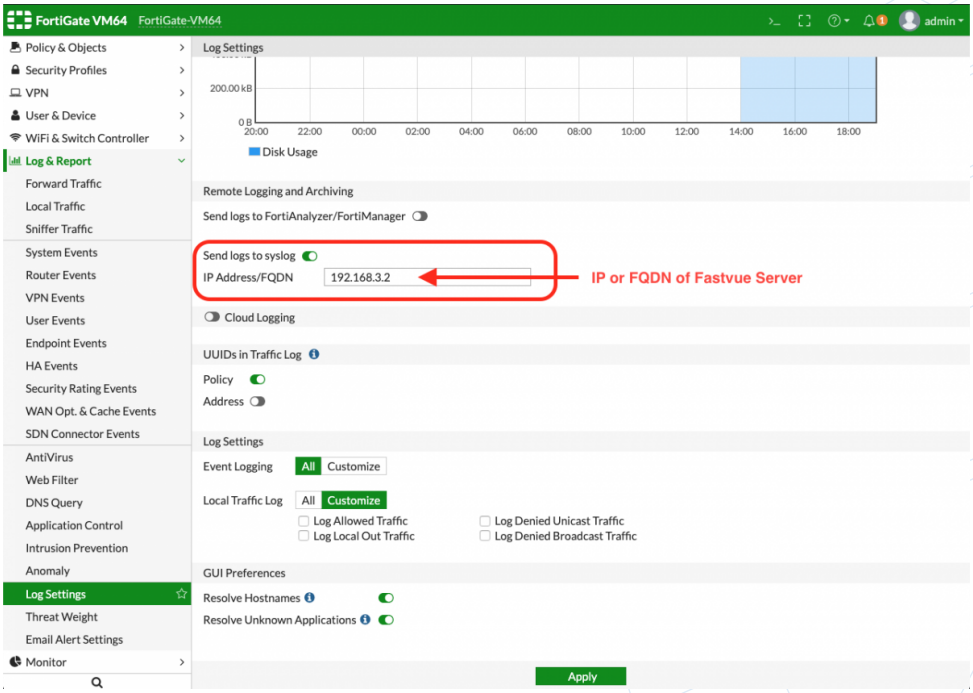
- **Data Location** (defaults to C:\ProgramData\Fastvue\Reporter for FortiGate). This is the location where all imported data, configuration and report files are stored. Specify a location with plenty of disk space.

2. Add the Fastvue Server as a Syslog Server in Fortinet FortiGate

Now that Fastvue Reporter for FortiGate has been installed, you need to add configure your Fortigate to send syslog data to the Fastvue server. To do this you will have to log a job with Customer service centre, [Home - ICT Self-Service Hub (service-now.com)]

Ask them to add the Fastvue Server as a Syslog Server using the FortiGate GUI:

1. In FortiGate's web interface, go to **Log & Report | Log Settings**
2. Scroll down to the **Remote Logging and Archiving** section and toggle the **Send logs to syslog** option to **on**
3. Enter the **IP** of the Fastvue Server into the edit box.
4. Scroll down and click **Apply** to save the settings.



Or add the Fastvue Server as a Syslog Server using the FortiGate CLI.

Log into the CLI and enter the following commands:

```
config log syslogd setting
        set facility user
        set port 514
        set server {IP or FQDN of the Fastvue server}
        set status enable
        end
```

Also ask them to configure forward, local and anomaly traffic logging

These logging features should be enabled by default, but make sure forward and local traffic as well as anomalies are being logged with the following commands:

```
config log syslogd filter
        set forward-traffic enable
        set local-traffic enable
        set anomaly enable
        set severity information
        end
```

And **Configure logging of all urls and referrer urls**

```
config webfilter profile
        edit {Name of the web filter profile}
        set log-all-url enable
        set web-filter-referer-log enable
        set extended-log enable
        set web-extended-all-action-log enable
        end
----repeat for all web filter profiles----
```

Your Fortigate will have 5 or 6 Webfiler Profiles that need to be edited.

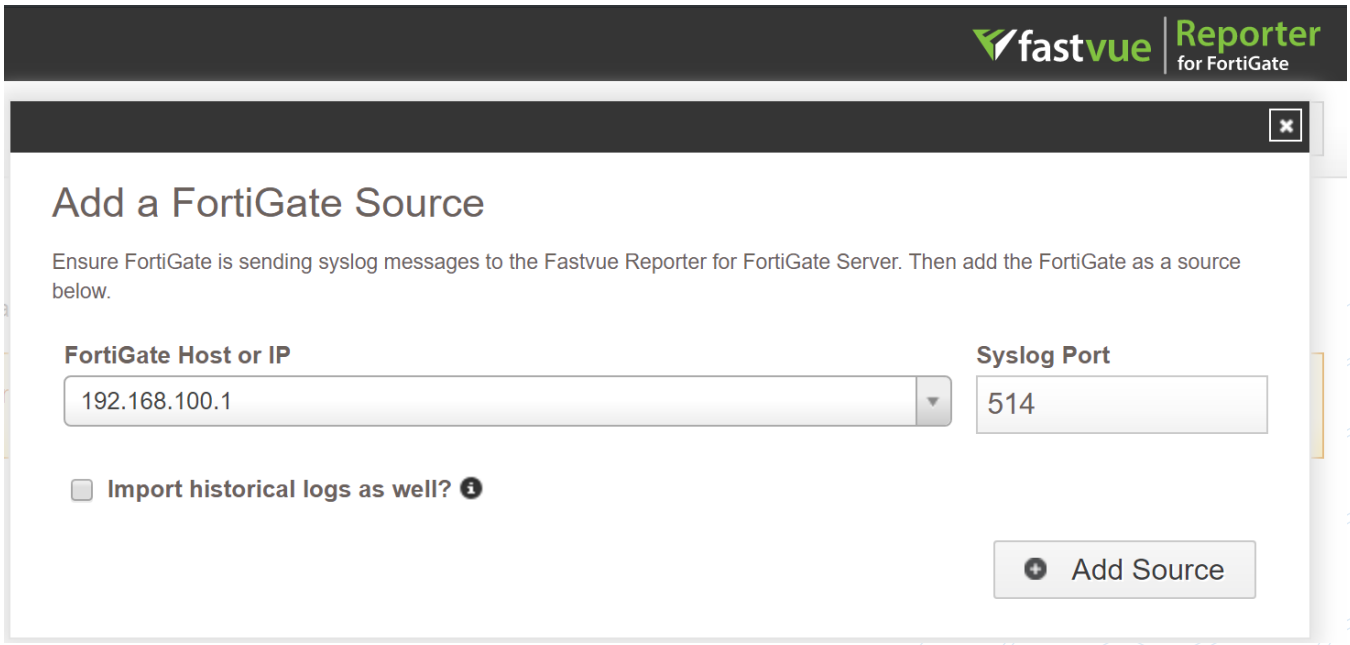
= Your Site Code

####-AllStudents,	####-AllStaff	####-BlockYouTube
####-YouTube	####-SocialBlock	####-AllVisitors

Once this has been done on the Fortigate you are ready to set your Fastvue server to receive the logs.

3. Add a Source

Add the FortiGate as a Source in Fastvue Reporter. This can be done on the start page that is presented after installation, or in **Settings** | **Sources** | **Add Source**.



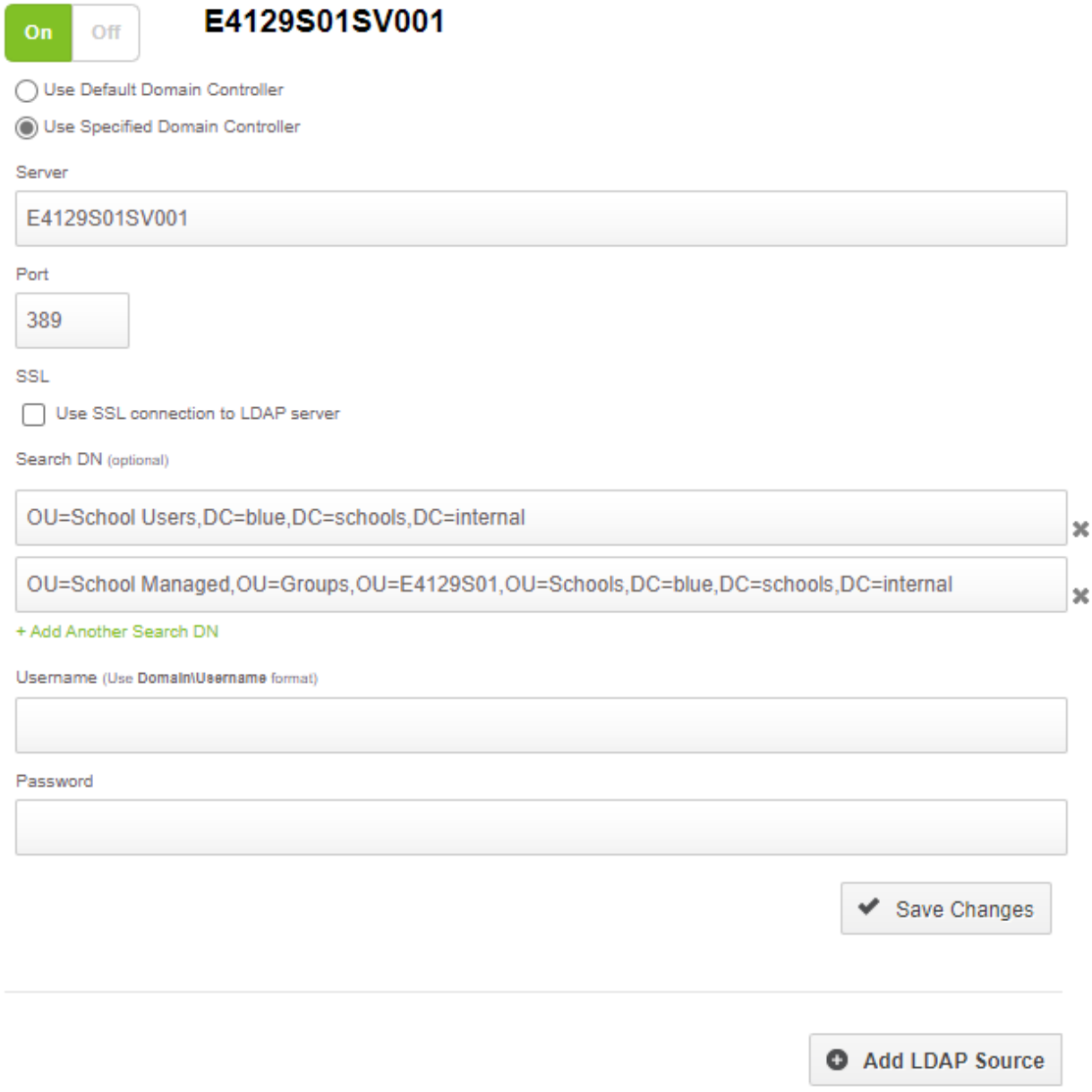
It may take 10-20 seconds before the first records are imported. You can watch the records and dates imported in **Settings** | **Sources**. Once records start importing, you can go to the Dashboard tab to see your live network traffic.

4. Directory / LDAP settings

Active Directory Settings

The Fastvue Reporter for FortiGate server queries Active Directory on a regular basis to retrieve user and department information.

Tick "**Use Specified Domain Controller**"
Set the Server to your site RODC, ie. **E####S01SV001** (Where E#### is your school code)
leave the port unchanged (**389**)
See image



Search DN

Set this to:

OU=School Users,DC=[Your Domain Colour],DC=schools,DC=internal

Add another Search DN and add:

OU=School Managed,OU=Groups,OU=[School site code],OU=Schools,DC=[Domain Colour],DC=schools,DC=internal

Save the changes. It will take a while for Fastvue to sync all of the users and domains

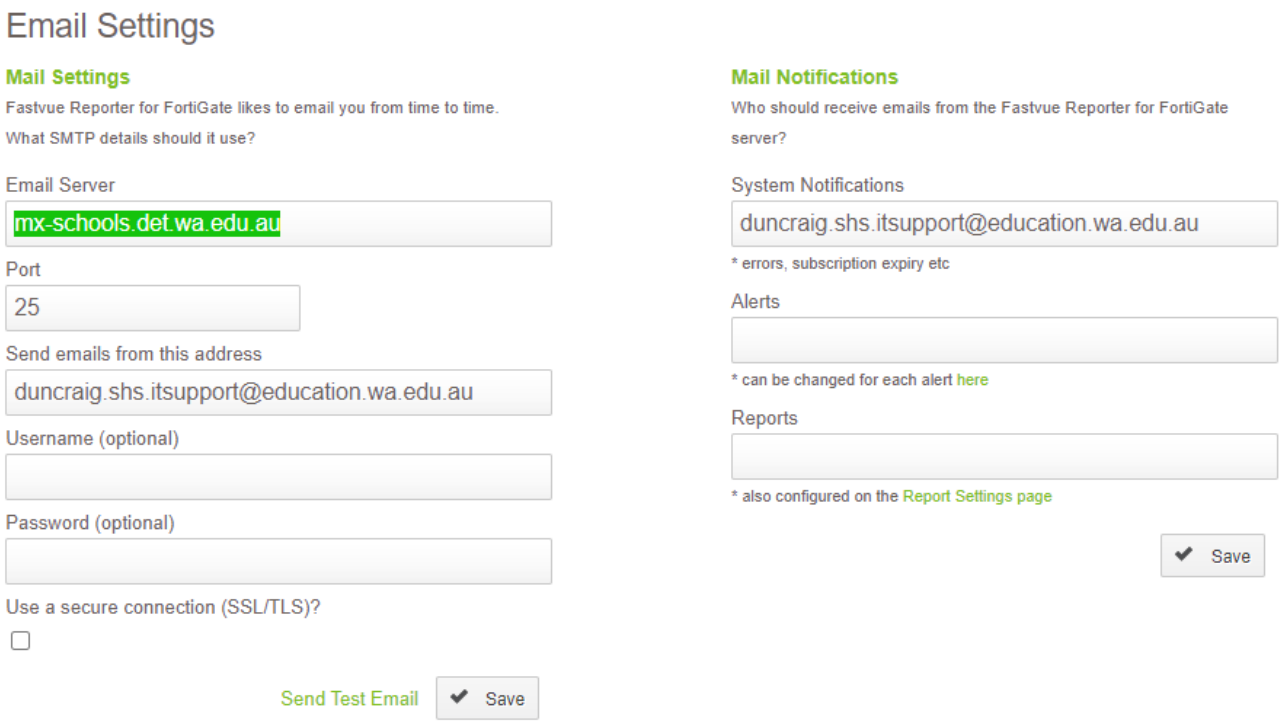
5. Email Settings

For best practice your school should always use a **distribution list** email address to send emails from. (*In the example you can see Duncraig SHS is using the IT Support email group*.)

Make sure you add one associated to your school. If you don't have one you can request one through the Service Desk - [Request Catalogue - ICT Self-Service Hub (service-now.com)]

Email Server:
mx-schools.det.wa.edu.au
Port:
25

Click on the "Send Test Email" to make sure your setting are correct and then [Save]



You can configure Mail Notifications here too. The example has "**Errors and System faults**" configured. But we leave the "**Alerts**" and "**Reports**" as they can be better configured under the Alerts and Reports tabs in Fastvue

6. Secure the Fastvue Reporter interface with login credentials!

You can secure the Fastvue Reporter site to administrators, and allow others to simply view reports, using Windows Authentication and Authorization rules in IIS.

Enable Windows Authentication

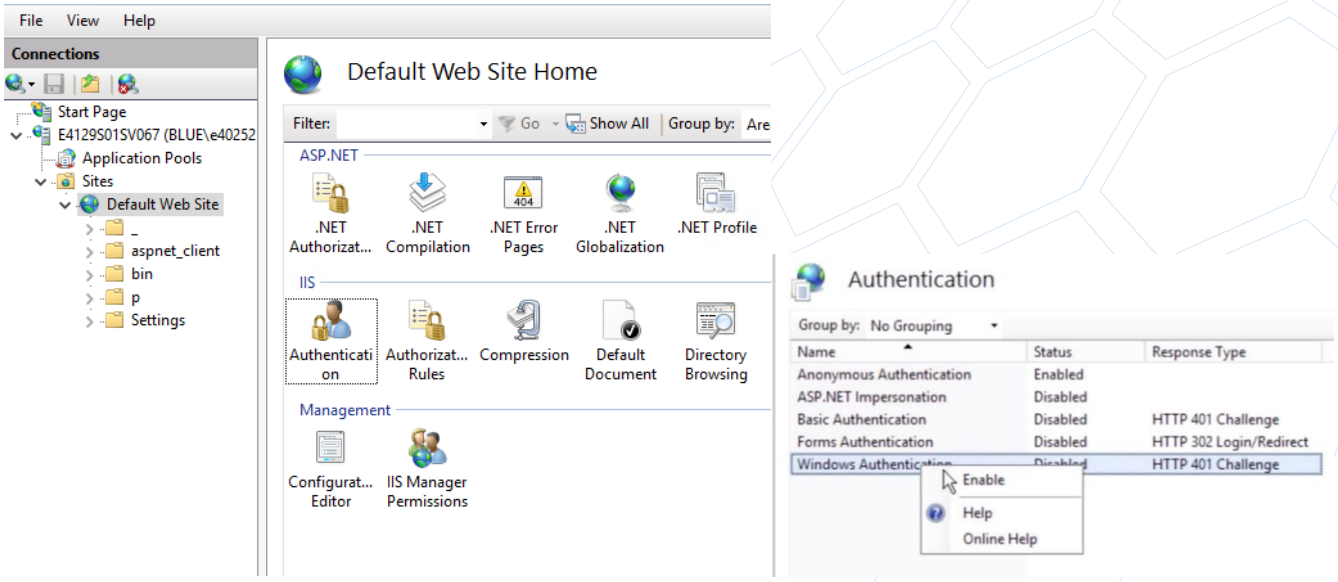
We need to enable IIS to Authenticate visitors to the Fastvue Reporter site using **Windows Authentication**.

We can use DAM groups on the Fastvue Server. One for **Admins** and another for **Viewers**. Fastvue Admins should contain anyone that needs full access to the entire application, and Fastvue Viewers should contain only people that need to view reports.

For the Admin group we will use: **E####S01-IntranetAdministrators.** And for the Viewers group we'll use: **E####S01-AdministrationStaff** & **E####S01-TeachingStaff.** You may want to use different DAM groups in you Viewer group but we will use these in our example.

To do this:

1. Go into **IIS Manager**, and select the **Fastvue Reporter** site or virtual directory.
2. Ensure 'Features' view is selected at the bottom of the middle pane and double-click **Authentication**.
3. Right click 'Windows Authentication' and select **Enable**. (If Windows Authentication is not in the list, you need to add the 'Windows Authentication' Role Service in **Server Manager | Web Server (IIS) | Role Services**).

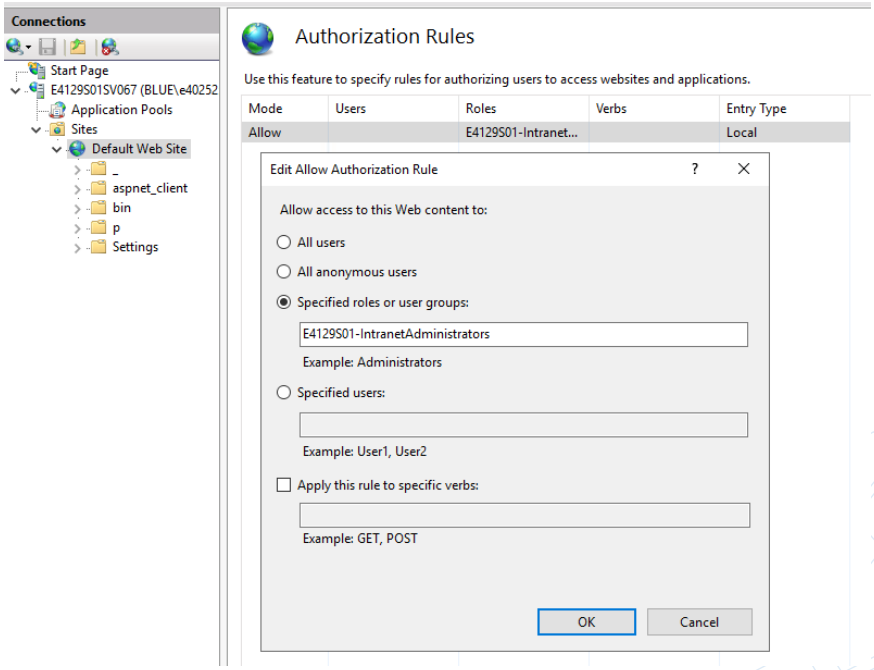


Add Authorization Rule for Admins

Now you need to add an authorization rule to allow the **Fastvue Admins** group to the entire website

To do this:

1. Select the Fastvue site or virtual directory on the left to return to the IIS features view, then double-click **Authorization Rules.** If Authorization Rules is not in the list, you need to add the 'URL Authorization' Role Service in **Server Manager | Web Server (IIS) | Role Services**).
2. Delete the rule to allow All Users, and add a rule to **Allow** the **Admins** group. In our case the **[E4129S01-IntranetAdministrators]** group from DAM

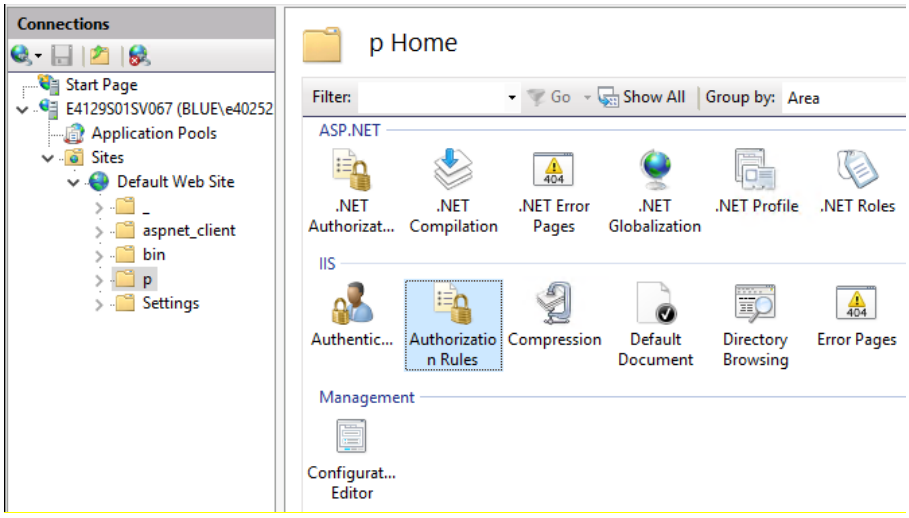


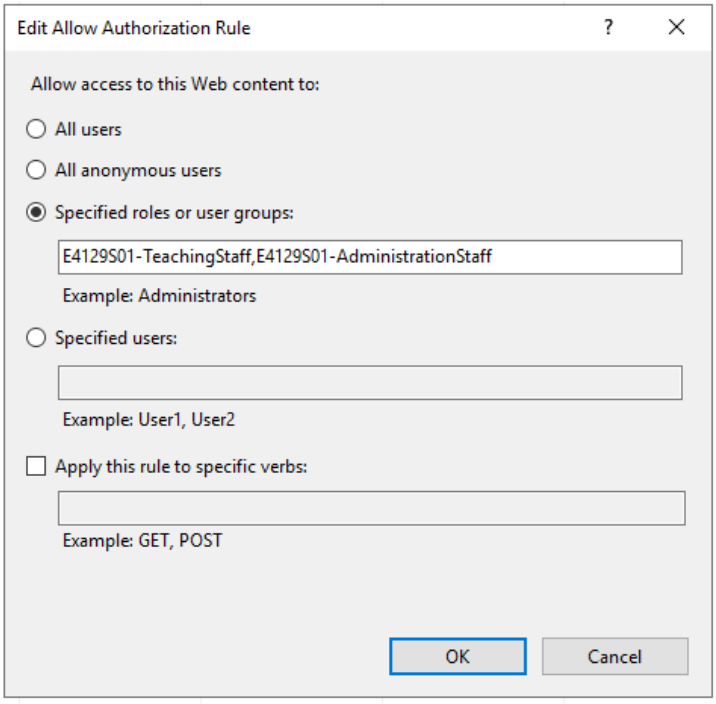
Add Authorization Rules for Report Viewers

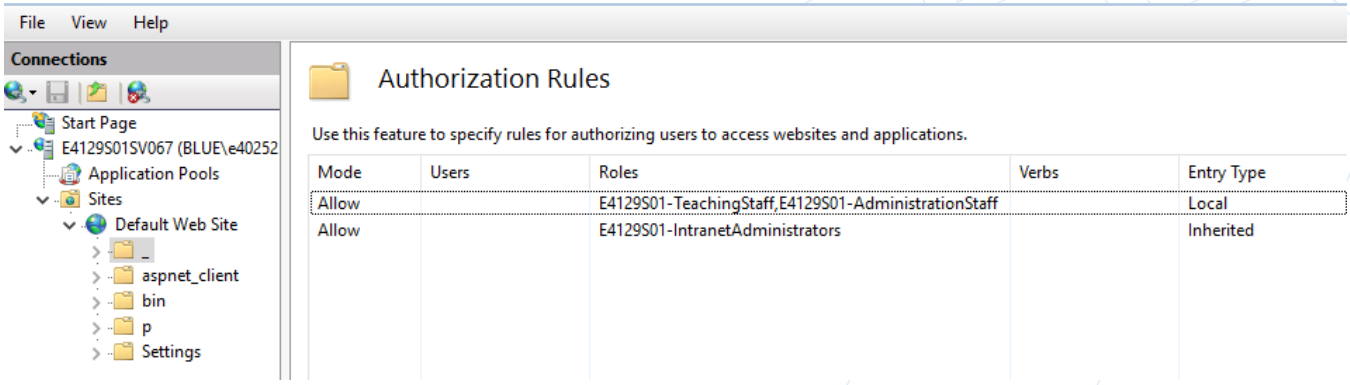
Now you need to add authorization rules to allow the **Viewers** group access to the **/p** and **/_** folders within the Fastvue Reporter website.

*Why? When you share a report using the 'Private Link' option, it gets shared from within the **/p** folder. Access to the /_ (underscore) folder is also required, as it includes the script files and other assets that are required for the Fastvue Reporter site to function.*

1. Open the Fastvue Reporter site on the left hand side and select the **/p** folder. Double-click **Authorization Rules** and add a rule to **Allow** the **Viewers** groups. [***E4129S01-AdministrationStaff,E4129S01-TeachingStaff***]
2. Select the **/_** (underscore) folder in the Fastvue Reporter website. Double-click **Authorization Rules** and add a rule to **Allow** the **Viewers** groups.


Connections
Start Page
E4129S01SV067 (BLUE\e40252
Application Pools
Sites
Default Web Site
_
aspnet_client
bin
p
Settings
p Home
Filter:
Go
Show All
Group by: Area
ASP.NET
.NET Authorizat...
.NET Compilation
.NET Error Pages
.NET Globalization
.NET Profile
.NET Roles
IIS
Authentic...
Authorizatio n Rules
Compression
Default Document
Directory Browsing
Error Pages
Management
Configurat... Editor


Edit Allow Authorization Rule
Allow access to this Web content to:
All users
All anonymous users
Specified roles or user groups:
E4129S01-TeachingStaff,E4129S01-AdministrationStaff
Example: Administrators
Specified users:
Example: User1, User2
Apply this rule to specific verbs:
Example: GET, POST
OK
Cancel

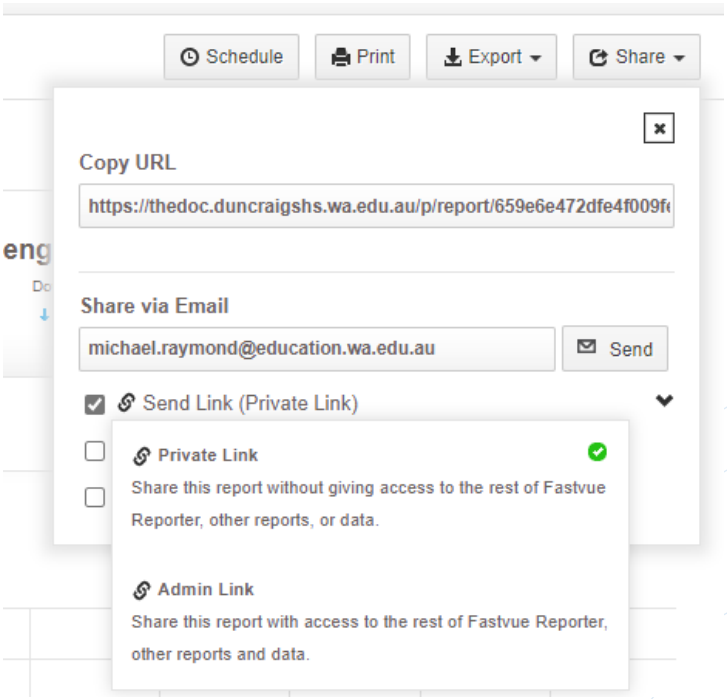

File View Help
Connections
Start Page
E4129S01SV067 (BLUE\e40252
Application Pools
Sites
Default Web Site
_
aspnet_client
bin
p
Settings
Authorization Rules
Use this feature to specify rules for authorizing users to access websites and applications.
Mode Users Roles Verbs Entry Type
Allow E4129S01-TeachingStaff,E4129S01-AdministrationStaff Local
Allow E4129S01-IntranetAdministrators Inherited

Test

If you're logged into Windows with a user account from an **Admins** group, you'll still be able to access the entire Fastvue Reporter interface. If not, you'll be prompted for authentication details, and denied access if the credentials supplied are not in the **Admins** group.

If you have a Private Report link, and you are logged into Windows with a user account in the **Viewers** group, you'll be able to access the report, as well as hover over items and run further reports. The secondary reports they will always bound by the data set of the original report. In other words, if you have received a report filtered by your department, you won't be able to run reports on anyone outside of your department or on any other data.

You can find the Private Link option when sharing and scheduling reports.



Now you can explore all the features of Fastvue Reporter for FortiGate.