

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Generate a Support Report from a Cisco Video Surveillance Server](#)

[Using the GUI](#)

[Using the CLI](#)

[Related Information](#)

Introduction

This document explains how to collect a support report from a Cisco Video Surveillance Server (VSM) 7.x

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on the Cisco Video Surveillance Server 7.x

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

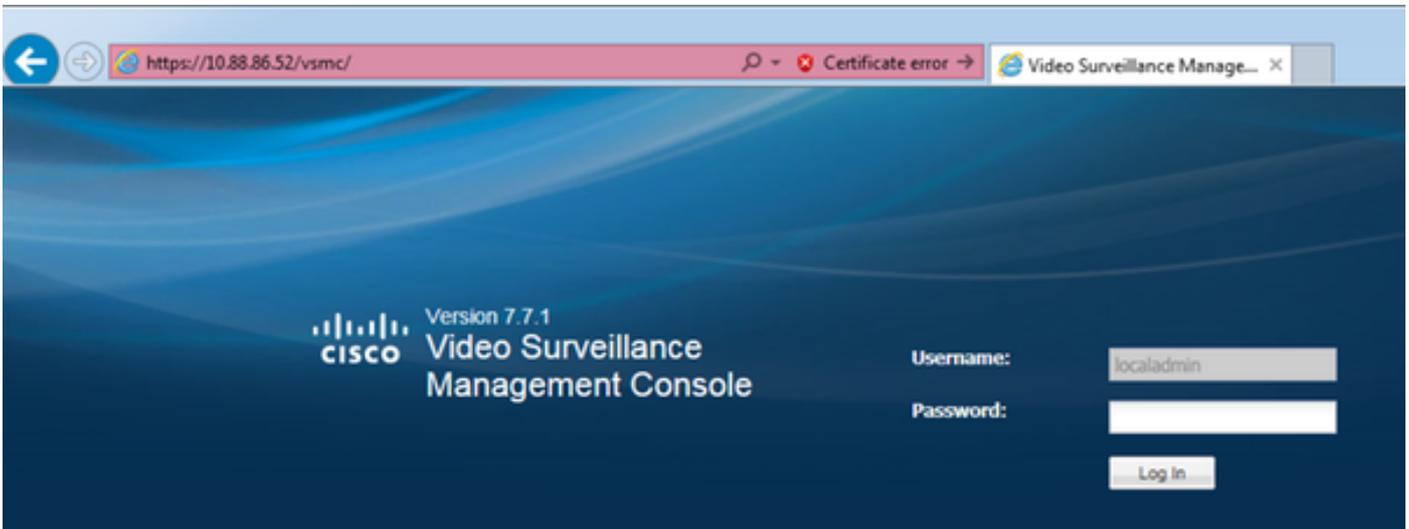
Generate a Support Report from a Cisco Video Surveillance Server

Support reports contain detailed information about the server for use in troubleshooting and system analysis. These reports are used by your support representative and should be generated only when requested

The support report can be generated either using the CLI or the GUI of the VSM server

Using the GUI

Step 1. Login to the Video Surveillance Server's management console page using - `https://<VSM ServerIP>/vsmc/`



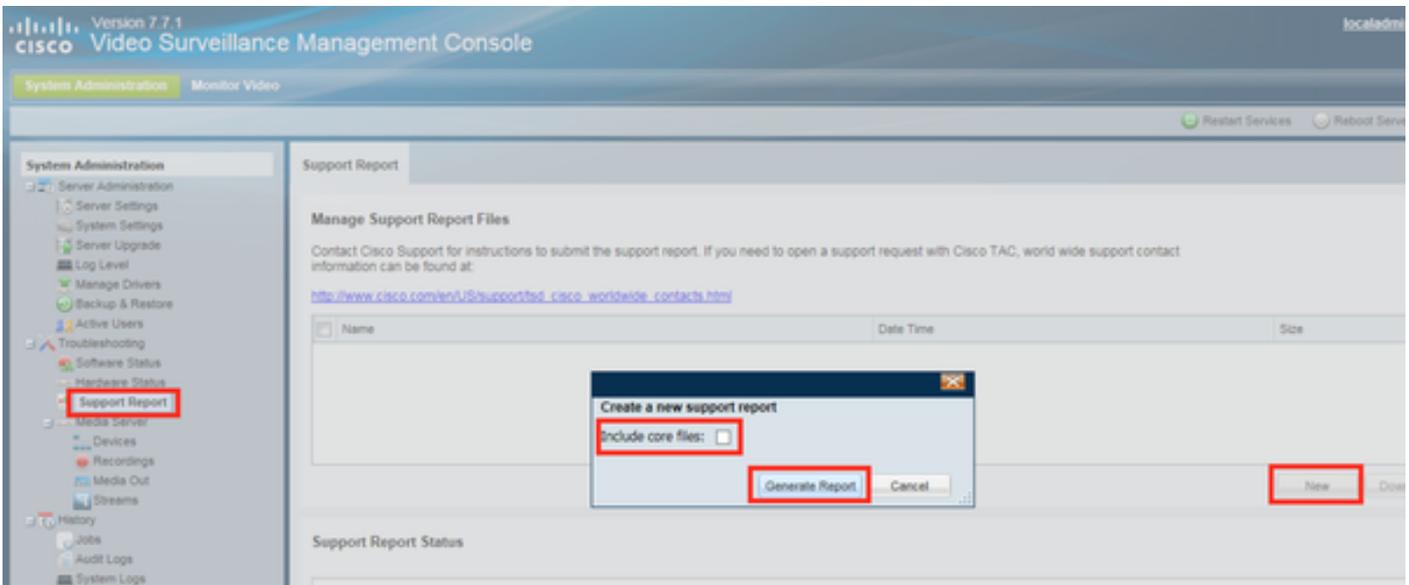
Alternatively on a Video Surveillance Operations Manager server login to the server and under the Operations Tab select 'Management Console'. This will open up the Management Console for the server where you can login with the 'localadmin' account.

Step 2. Select Support Report

Step 3. Click New

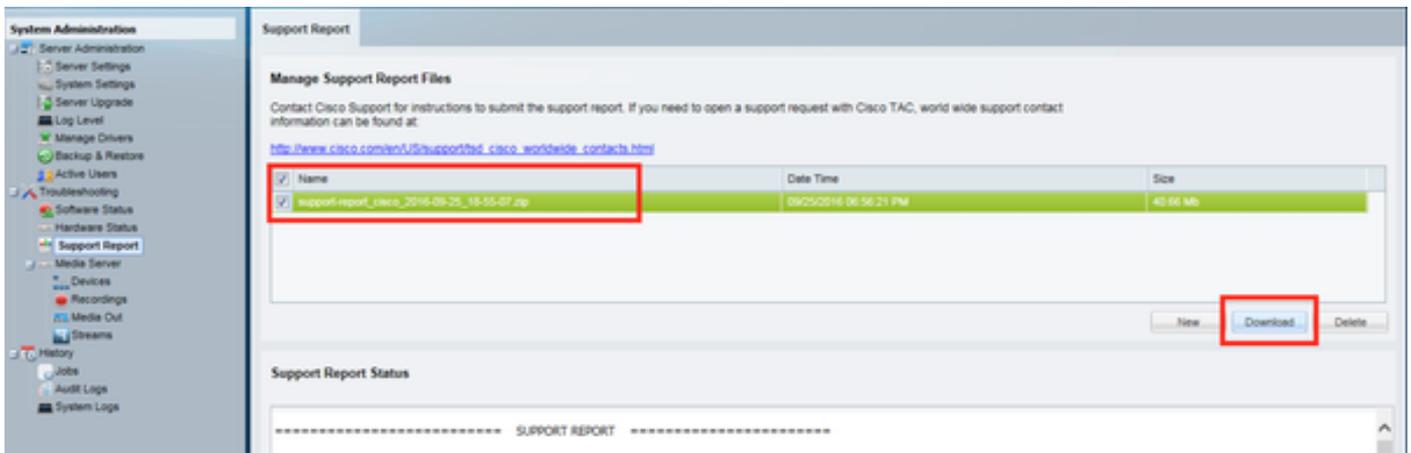
Step 4. If you are troubleshooting issues involving server crashes click on Include Core Files. If not leave the option unchecked

Step 5. Click Generate Report to create a new support report



Step 6. Wait for the report to be generated

Step 7. Select the report and click Download



Using the CLI

In many cases the GUI of the server may not be accessible , in such cases the support report can be generated using the CLI

Step 1. Establish a secure shell (SSH) session to the Cisco Video Surveillance server using an application such as putty, and authenticate with the localadmin account

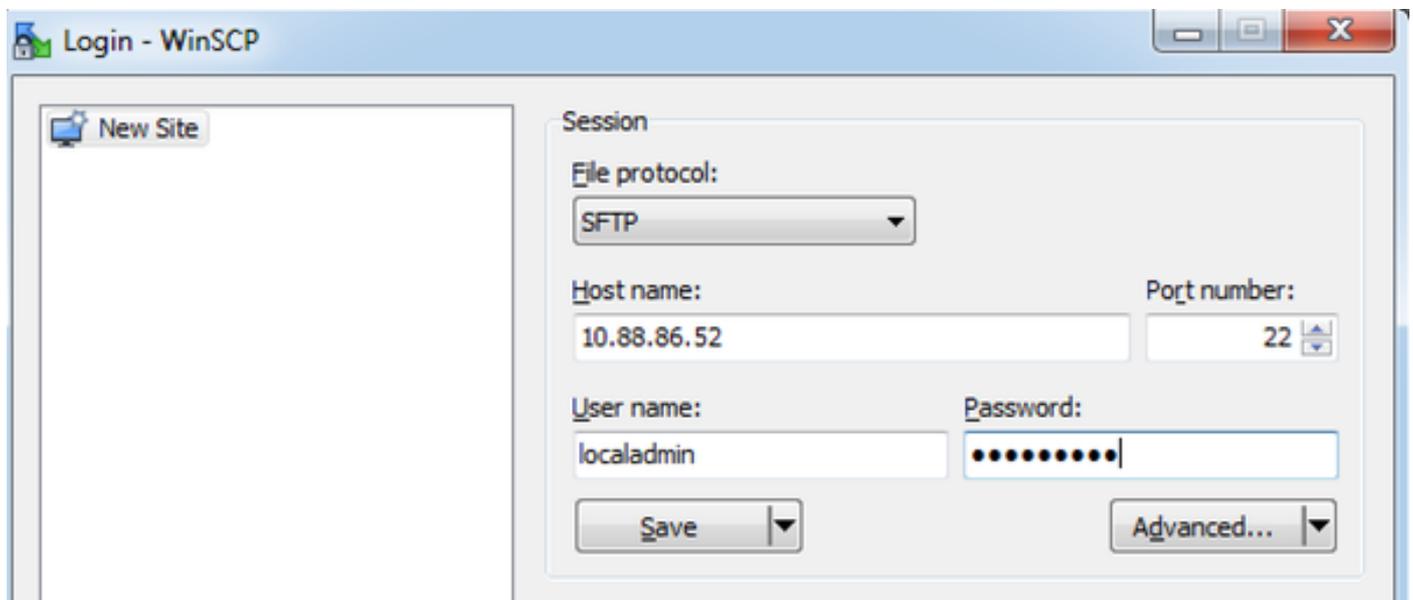
Step 2. Run the command **sudo su -** to change to super user mode

```
root@cisco:~  
login as: localadmin  
localadmin@10.88.86.52's password:  
Last login: Sat Sep 24 15:20:47 2016 from 10.24.128.164  
[localadmin@cisco ~]$ sudo su -  
[root@cisco ~]# █  
  
█
```

Step 3. Run the command **support-report** and wait for the report to be generated

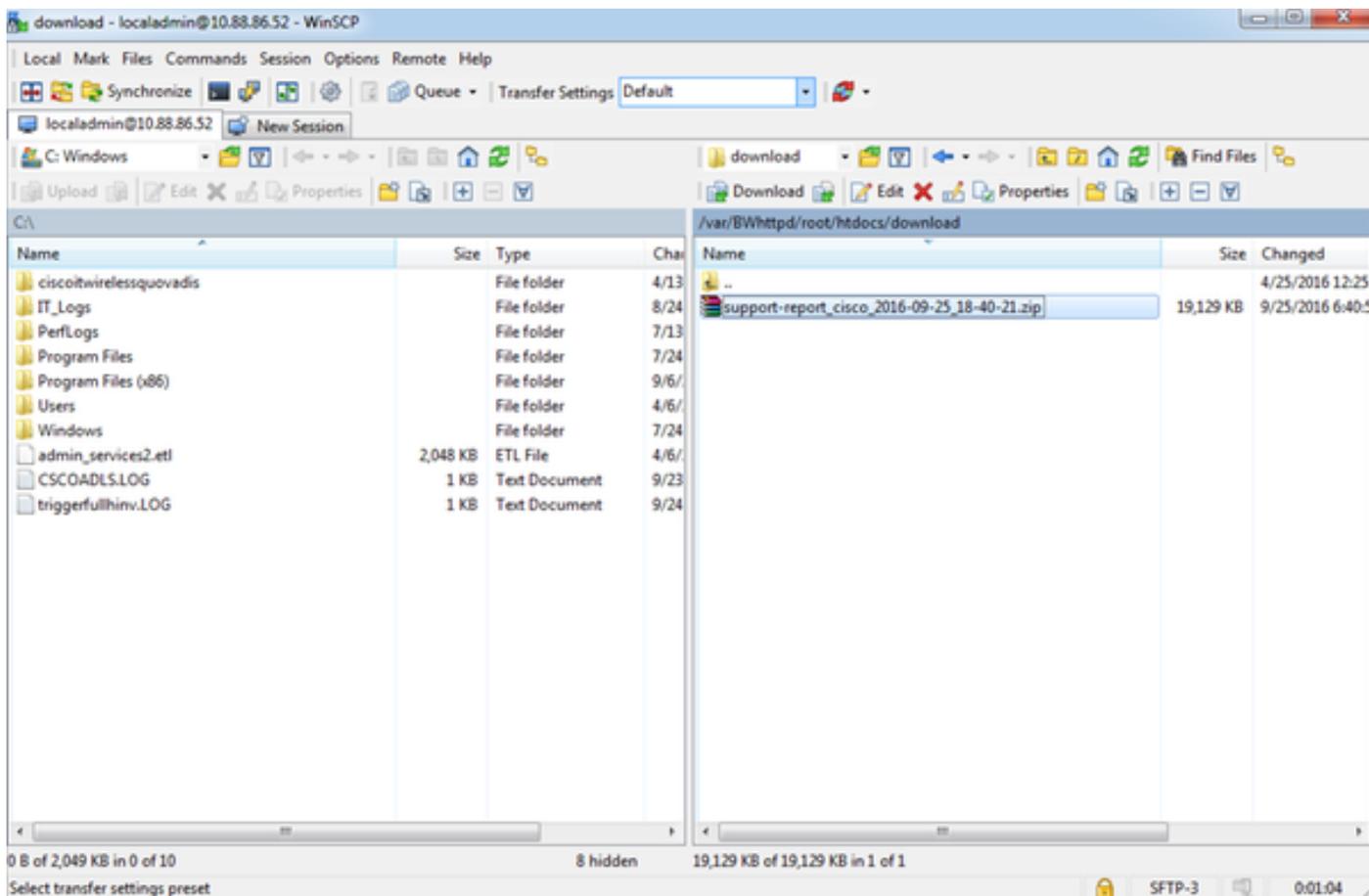
```
[root@cisco ~]# support-report
Generating report...
Building system configuration...
Collecting Storage Monitoring Data...
/usr/BWhttpd/bin/reposdbtestclient: error while loading sha
1.so.1.0.0: cannot open shared object file: No such file or
Checking for database server ... Running.
Checking for VSOM database server ... Running.
Checking for VSOM database server ... Running.
Checking for VSOM database server ... Running.
ERROR 1049 (42000): Unknown database 'vsf'
done!
Building package list...done!
Building process list...done!
Reading open files... done!
Copying hardware profile...done!
Copying system logs...Done!
Copying VS logs...
File to convert deviceUID :/usr/BWhttpd/logs/ims.log:
Copying device-uid name mapped ims log ...
```

Step 4. Establish a Secure File Transfer Protocol (SFTP) session to the server using an application such as WinSCP, and authenticate with the localadmin account



Step 5. Navigate to the `/usr/BWhttpd/root/htdocs/download/` folder on the server

Step 6. Drag and drop the file from the server onto the desired location on your workstation



Related Information

If the logs were requested by a Cisco TAC Engineer , they can be uploaded to the TAC case using one of the methods outlined in the below document

<http://www.cisco.com/c/en/us/about/security-center/tac-customer-file-uploads.html>

Here is a link to a video explaining how to capture the support report using the GUI

<https://www.youtube.com/watch?v=oDSAZjUzalc>