Initial Configuration Guide for Content Analysis Virtual Appliance High-Performance Models

CA Version 2.4

Symantec

Legal Notice

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

www.symantec.com

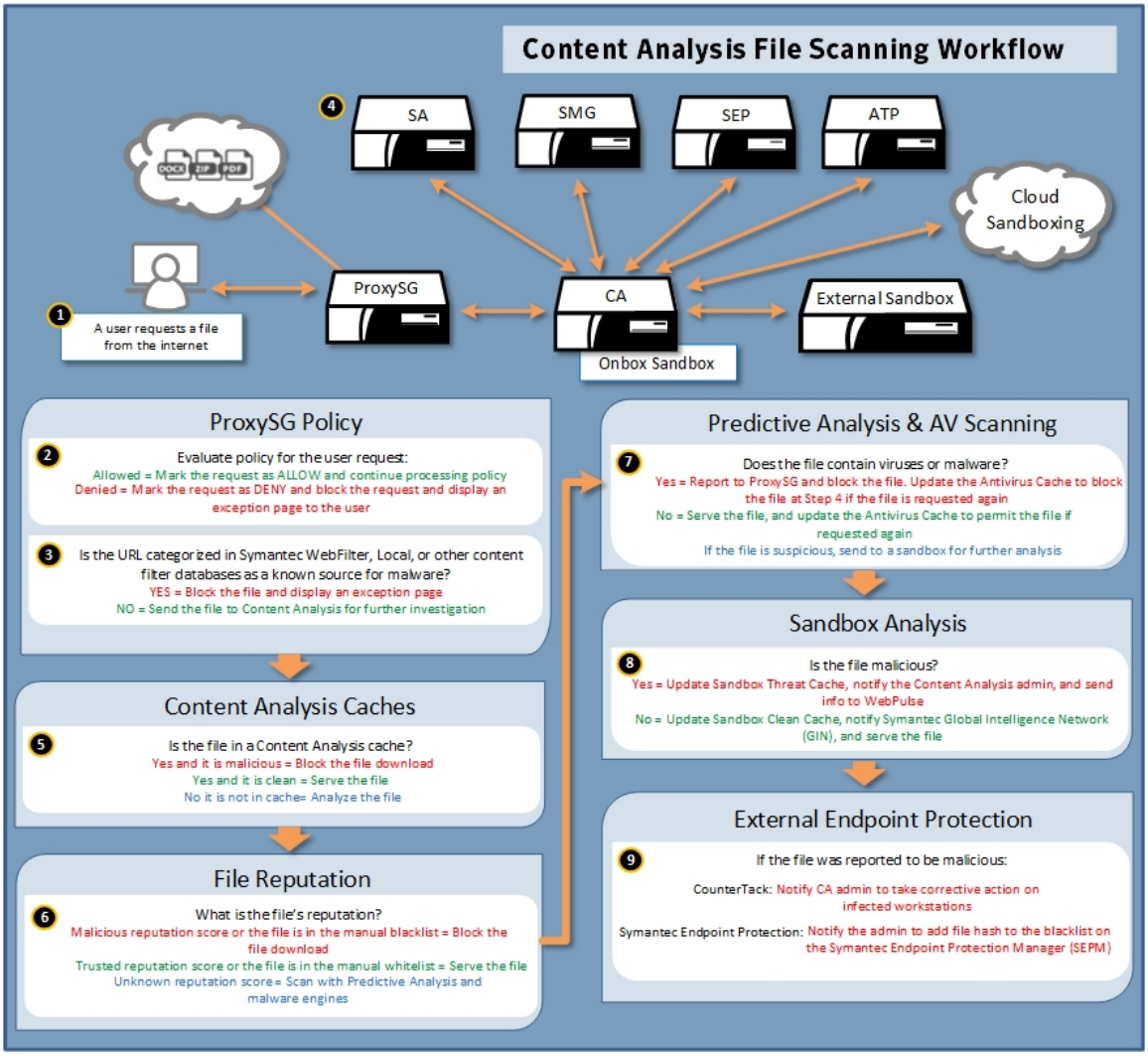
Tuesday, December 17, 2019

Table of Contents

Introduction to Content Analysis

Symantec Content Analysis is a next-generation antivirus, malware, and spyware detection system. Content Analysis 2.4 includes the following features:

- **Malware and Antivirus Scanning** — Content Analysis supports Symantec, Kaspersky, McAfee, and Sophos antivirus engines and virus signature databases. You can use one or two AV engines with Content Analysis.
- **Predictive Analysis** — Optional subscription services from Symantec and Cylance use an advanced artificial intelligence engine to identify malware.
- **File Reputation Service** — Content Analysis generates SHA1, MD5, and SHA-256 hashes for each file it processes. These hashes are compared with Symantec's cloud-based File Reputation classification service to identify known files. The service uses reputation scores, numbers (**1**–**10**) that indicate whether files are known to be trusted or malicious; low scores are less likely to be threats whereas high scores are more likely. Depending on the reputation score, files are then either blocked if the score is high, passed to the user as safe if the score is low, or processing continues with anti-virus scanning and sandboxing if the service doesn't know whether the file is malicious.
- **Manual File Blacklist and Whitelist** — As your organization identifies files that are known good or bad, you can add them to a list of manually defined file hashes to either allow or deny those files without further processing.
- **Sandbox Integration** with external vendors (Symantec Malware Analysis, Lastline, or FireEye) — Sandbox services use different methods to identify the actions an executable file would take on a client workstation, including malicious URL web requests and changes to system files.
- **Endpoint Integration** — As the sandbox detects malware, Content Analysis can query a CounterTack Sentinel server in your network to determine which users (if any) have retrieved it. If Symantec Endpoint Protection Manager (SEPM) is integrated with Content Analysis, the administrator is notified when the sandbox finds a malicious file and provides an option to add the file hash to a blacklist on the SEPM.
- **Cached Responses** — When a Content Analysis module determines a verdict (clean vs. malicious) for a file, it will cache the file hashes and verdicts to avoid having to scan the same file on subsequent requests. Content Analysis has separate caches for responses from each of its services: antivirus, file reputation, predictive analysis, and sandboxing (threats and clean).
- **Symantec Global Intelligence Network (GIN)** — Users are protected by the Symantec WebFilter and GIN databases on the ProxySG appliance, and when malware is discovered through scanning, those results can be shared with WebFilter to classify bad URLs for the benefit of all GIN users worldwide.



1. A user in the protected network requests a file from the Internet.
2. The ProxySG appliance evaluates policy for the user's request, and allows or denies the request according to policy.
3. The ProxySG appliance compares the file against the Symantec WebFilter and GIN databases. If the domain hosting the file has been categorized as a malware source, the file download is denied and the user is notified. If the domain is not recognized, the file is sent to Content Analysis for inspection.
4. Other Symantec solutions such as Security Analytics, Secure Message Gateway, Symantec Endpoint Protection, and Advanced Threat Protection can send files to Content Analysis for analysis.
5. Content Analysis looks for the file hash in each of its caches (Antivirus, File Reputation service, Predictive Analysis, and Sandboxing). If the hash is located in a cache, Content Analysis either serves or blocks the file based on the verdict.

6. Content Analysis compares the file details against the both the manual blacklist/whitelist and the Symantec File Reputation service. If the file's hash is on the blacklist or results in a malicious reputation score, the file is blocked. If the file's hash is on the whitelist or results in a reputation score that is trusted, scanning is suspended and the file is sent to the user. If the file's reputation score is unknown or the hash is not on the whitelist or blacklist, the file is compared against the virus scan cache. If not present, the file is forwarded to the enabled antivirus scanners.
7. The file is examined by optional predictive analysis services (Symantec Advanced Machine Learning and/or Cylance), and then scanned by the configured antivirus engines for known virus signatures. If the file contains malware, the file is blocked and the user receives a deny page with a description of the virus or malware.
8. If the file is clean, but is of a suspicious type (such as an executable or a type defined in the sandboxing configuration), it is simultaneously sent to the user and forwarded to an external sandbox appliance/service or Symantec Cloud Sandboxing for further analysis. (If you prefer real-time sandboxing for a particular file type, you can select the **Wait for Result** option when configuring general sandbox settings.) The results of the sandbox analysis are reported to the administrator and shared with Symantec GIN. If the file is malicious, the Content Analysis administrator is notified via email or other configured notification method.
9. If endpoint integration is configured on Content Analysis and the sandbox analysis found the file to be malicious, Content Analysis queries the endpoint manager (Symantec Endpoint or CounterTack Sentinel) to determine if any workstations in the network have been infected. That information is then included in the report emailed to the administrator. If Symantec Endpoint Protection Manager (SEPM) is configured, Content Analysis notifies the administrator, providing the option to add the file hash to a blacklist on the SEPM.

Recommended Reading

Before you set up your set up your Content Analysis Virtual Appliance for the first time, Symantec recommends that you review the following documentation:

- VMware Documentation, for assistance with setting up your virtualization environment: http://www.vmware.com/support/pubs/
- Symantec Product Documentation, for Content Analysis: https://support.symantec.com/en_US/Documentation.html
- *SymantecContent Analysis Release Notes*, which contains information on third-party requirements, known issues, and other important information for setting up Content Analysis whether as part of an on-box solution or as a virtual appliance. Release notes are available when downloading an image.

Terminology

Important terms used in Symantec documentation are listed alphabetically in the following table.

In some cases, this document uses abbreviations instead of expanded forms. While using this document, refer to this table to determine the meaning or expanded form of a term.

Term	Description and Usage
Command Line Interface (CLI)	One of two ways to access Content Analysis; a command line tool where you can execute administrative commands. See "Log onto the CLI" on page 25.
Open Virtualized Format (OVF)	A format for packaging and distributing virtual machines. The OVF file in the VAP is an XML text file that defines the attributes of the specific virtual machine package.
Serial Number	A string of numbers that uniquely identify an appliance. When you first power on the VA, you must enter the serial number to begin initial configuration.
Virtual Appliance (VA)	The virtual machine image.
Virtual Appliance Package (VAP)	The zip file that contains the OVF file and the virtual disk files (.vmdk) required for creating the Virtual Appliance.
Virtual Machine (VM)	An instance of an operating system and one or more applications that run in an isolated partition of a VMware server.
VMware client	The virtualization software used to create and/or host the virtual appliance. For simplicity, this document uses the term **VMware client** in all instances; substitute it with the supported ESX host you are using.
Web management console (Content Analysis UI)	One of two administration methods; you display the web interface in a browser window, and it is the main point of access for performing tasks. See "Access the Web Management Console" on page 22.

Access Symantec Documentation

- Access the Content Analysis WebGuide and other documentation on https://support.symantec.com/content/unifiedweb/en_US/Documentation.1145459.html.
- Release notes are available when downloading the image. Go to https://www.symantec.com/support-center/getting-started and follow the prompts to get to the image download.

Contact Us

We appreciate your comments. Please comment on specific errors or omissions, accuracy, organization, subject matter, or completeness of this guide. To send feedback on this or other Symantec product documentation, write to us at documentation_inbox@symantec.com.

Verify System Requirements

To achieve the best performance on the CA VA, it is important that you install the software on a system that meets the specified requirements. Follow these guidelines to guarantee satisfactory performance and operation of the CA VA.

> **Note:** The following requirements reflect Symantec 's test environment. Using the same or a similar configuration should achieve satisfactory performance of the CA VA; however, you should expect different performance results if your resources or virtual drive configuration are different from the configuration described in Table 2–1 and Table 2–2. Be aware that over-provisioning CPUs and memory cause license suspension, but under-provisioning can cause sub-optimal VA performance and operation.

Table 1: General System Requirements

Resource	Requirement
VMware versions **Note:** Your VMware license must be Enterprise or Enterprise Plus if you want to use remote serial connections.	VMware ESX Server 5.5, 6.0, or 6.5
Virtual CPU **Note:** You must reserve at least the minimum CPU. See "Reserve Resources for the CA VA"	1 GHz (minimum); 2.6 GHz (recommended)
Minimum storage space per drive	100 GB

The table below lists requirements for each model. Symantec recommends creating 100GB virtual drives, although models with higher storage requirements can have larger drives.

> **Note:** The OVF template contains two virtual disk files (VMDK). The smaller disk is used for boot only.

Table 2: Model-Specific Requirements

Model	Virtual CPUs	Virtual Memory (GB)	Total Storage (GB)	Recommended Virtual Drive Configuration	Estimated Throughput Mbps* 1 vs 2 AV		Recommended ProxySG VA Model
CAS-VA-C4S	4	8	100	1x100GB	100	100	C1S(1x4)
CAS-VA-C4M	4	12	100	1x100GB	100	100	C1M(1x6)

Model	Virtual CPUs	Virtual Memory (GB)	Total Storage (GB)	Recommended Virtual Drive Configuration	Estimated Throughput Mbps* 1 vs 2 AV		Recommended ProxySG VA Model
CAS-VA-C4L	4	16	100	1x100GB	100	100	C1L(1x8)
CAS-VA-C8S	8	16	100	1x100GB	200	200	C2S(2x8)
CAS-VA-C8M	8	24	100	1x100GB	200	200	C2M(2x12)
CAS-VA-C8L	8	32	100	1x100GB	200	200	C2L(2x16)
CAS-VA-C16S	16	32	100	1x100GB	400	400	C4S(4x16)
CAS-VA-C16M	16	48	100	1x100GB	400	400	C4M(4x24)
CAS-VA-C16L	16	64	100	1x100GB	400	400	C4L(4x32)
CAS-VA-C32S	32	64	200	1x200GB	800	500	C8S(8x32)
CAS-VA-C32M	32	96	200	1x200GB	800	500	C8M(8x48)
CAS-VA-C32L	32	128	200	1x200GB	800	500	C8L(8x64)
CAS-VA-C64S	64	128	200	1x200GB	1600	1000	C16S(16x64)
CAS-VA-C64M	64	192	200	1x200GB	1600	1000	C16M(16x96)
CAS-VA-C64L	64	256	200	1x200GB	1600	1000	C16L(16x128)

Note: *Throughput values are subject to change based on traffic mix and the virtual host hardware.

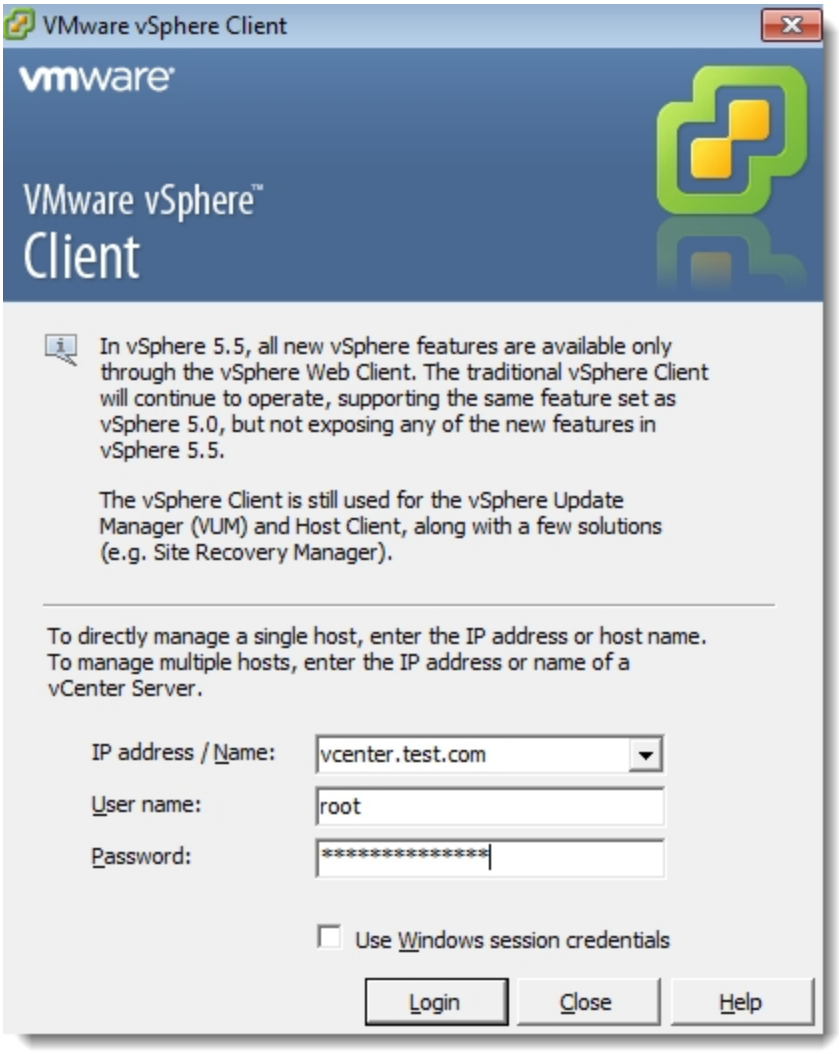
Verify Resource Availability

Because all virtual appliances use a hardware resource pool that can be shared and assigned as needed, you must verify that the vSphere Hypervisor meets the minimum hardware requirements for the CA VA model that you have purchased.

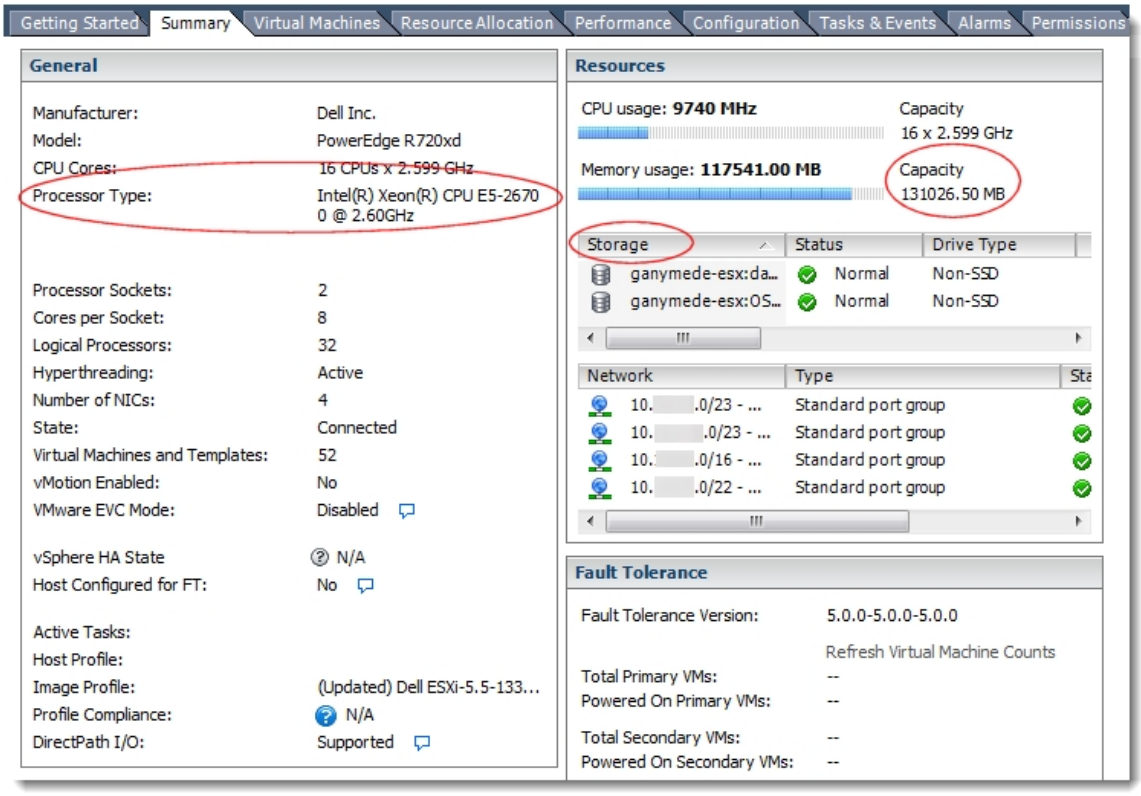
The following instructions describe how to verify system resources on the vSphere Hypervisor using a VMware client. The client is used to connect directly to a vSphere Hypervisor or indirectly to a vSphere Hypervisor through vCenter Server.

To verify resource availability:

1. Use your VMware client to log in to the vSphere Hypervisor.



2. To display the summary of the vSphere Hypervisor's resources, select the ESX server and click the **Summary** tab.



3. Verify adequate resource availability.

   a. In the **General** panel, confirm that the processor speed meets or exceeds requirements. See "Table 1: General System Requirements" on page 9.

   b. In the **Resources** panel, beside **Memory usage**, confirm that the memory **Capacity** meets or exceeds requirements of your CA VA model. For example, the CAS-VA-C16S requires 32 GB RAM. See "Table 2: Model-Specific Requirements" on page 9.

   c. In the **Resources** panel, in the **Storage** section, confirm that there is adequate free space on a local datastore on the vSphere Hypervisor to accommodate the disk requirements of your CA VA model. For example, the CAS-VA-C16S requires a total storage space of 100 GB.

Prepare for Initial Configuration

The initial configuration wizard prompts you to configure basic network settings. Record the information specific to your deployment in this table, and then use your notes for reference when you go through the installation process.

> **Tip:** Print out this table for reference.

Requirement	Description	My values
Appliance serial number	See "Retrieve Your Serial Number" on the facing page.	
Interface configuration	IP address	
	Subnet mask	
Default gateway	IP address for the default gateway	
DNS server	IP address for the primary DNS server	

Retrieve Your Serial Number

(missing or bad snippet)

Set Up Content Analysis

If you are using Content Analysis for the first time, perform the following steps to install and set up Content Analysis.

1. Download the VAP file from the Symantec Support site.
   See "Download and Extract the VAP File" on page 16.
2. Retrieve your serial number for the VA.
   See "Retrieve Your Serial Number" on page 14.
3. Import the OVF file to your VMware client to create the Content Analysis VA.
   See "Create the Virtual Appliance" on page 16.
4. Enter the valid serial number to activate Content Analysis.
   See "Enter Your Serial Number" on page 19.
5. Complete the steps in the initial configuration wizard to configure the Content Analysis VA.
   See "Configure the Virtual Appliance" on page 20.
6. Install the Content Analysis license.
   See "Install the VA Appliance Certificate and License" on page 22.
7. (Optional). Configure a proxy for Internet access.
   If your Content Analysis deployment requires that all traffic be processed by a ProxySG appliance, see "Configure Explicit Proxy" on page 24.

Download and Extract the VAP File

Log in to the Symantec Support site and download the Content Analysis Virtual Appliance Package (VAP) file. The VAP is a ZIP file that contains:

- An Open Virtualized Format (OVF) file
- Two Virtual Machine Disk Format (VMDK) files:
  - **CASMA-VA-disk1.vmdk** (for the boot disk)
  - **CASMA-VA-disk2.vmdk** (for the virtual disk)

1. Go to https://www.symantec.com/support-center/getting-started and follow the prompts to download the software.

> **Note:** The OVF file includes a pointer to the VMDK files; thus, you must extract and store the contents of the ZIP file within the same folder. Do not rename the files.

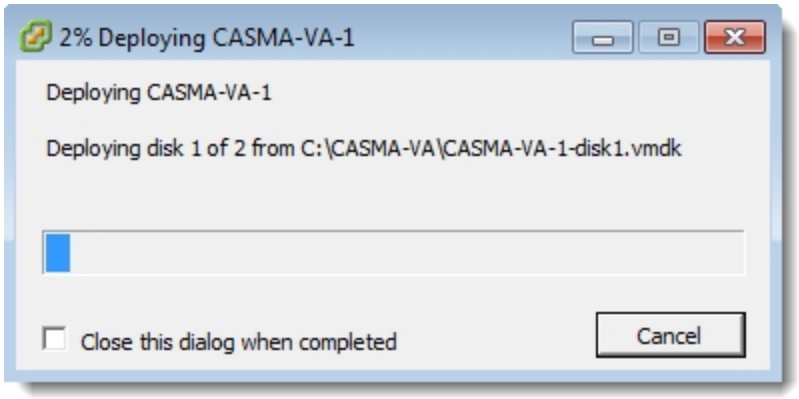
Create the Virtual Appliance

After you extract the files from the Virtual Appliance Package ZIP, create the virtual appliance by deploying the OVF template.

1. Create the CA VA on your host vSphere Hypervisor.
   a. In your VMware client, select your host vSphere Hypervisor.
   b. Select **File > Deploy OVF Template**. The *Deploy OVF* wizard begins.
   c. In the **Source** dialog, click **Browse** and browse to where you extracted the OVF file.
   d. Click **Next**.
   e. Verify the details for OVF template and click **Next**.
   f. In the **Name and Location** dialog, enter a name for the CA VA, such as **CAVA_Sydney**. (The default name is **CASMA-VA-1**). You should enter a name that is unique within your vSphere Hypervisor host.
   g. Click **Next**.
   h. In the **Disk Format** dialog, select a datastore with sufficient free space for your CA VA model. See "Table 2: Model-Specific Requirements" on page 9 for disk space requirements.
   i. Select one of the *thick* provisioning types for the virtual disk format and click **Next**.

j. On the **Ready to Complete** dialog, review your settings.

k. Click **Finish**. The VMware client displays a **Deploying <name>** message with a progress bar.



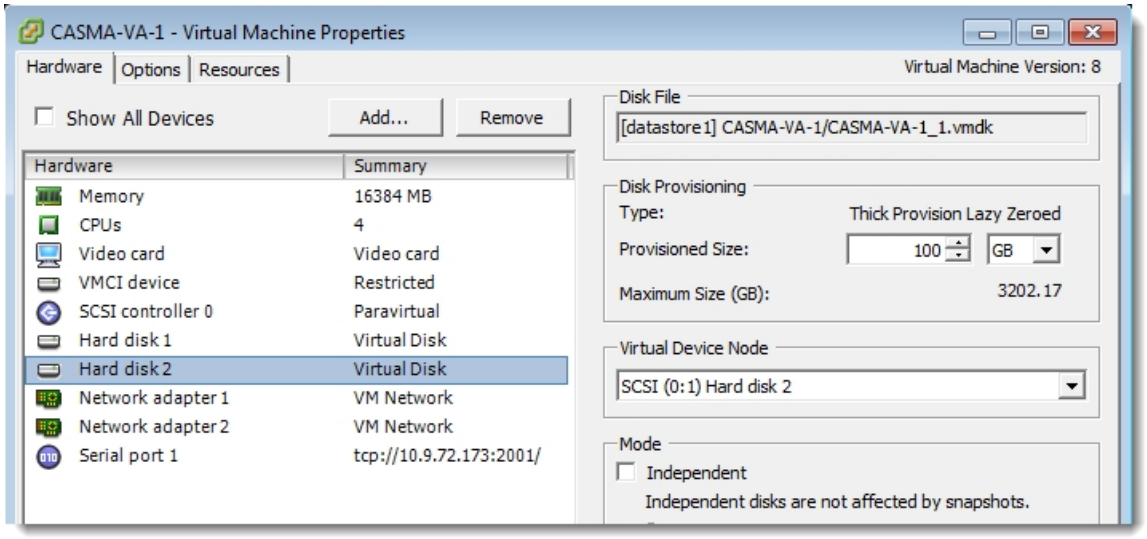
When deployment is complete, close the dialog. The inventory list on the left displays the new virtual machine.

2. Increase the size of your virtual disk, *if required for your CA VA model*. For example, the CAS-VA-C64L requires 200 GB of storage space so you must increase the disk size from 100 GB (the default size) to 200. See "Table 2: Model-Specific Requirements" on page 9.

a. Select the Content Analysis VM on the vSphere Hypervisor Server.

b. Right-click and select **Edit Settings**. The *Virtual Machine Properties* dialog opens.

c. In the **Hardware** tab, select **Hard disk 2**.



d. For **Provisioned Size**, enter **200**.

e. Click **OK**.

3. Make sure the VM is powered off, as the next step will work only on a powered-off VM.

   a. Right-click the Content Analysis VM in your inventory list, and select **Power > Power Off**.

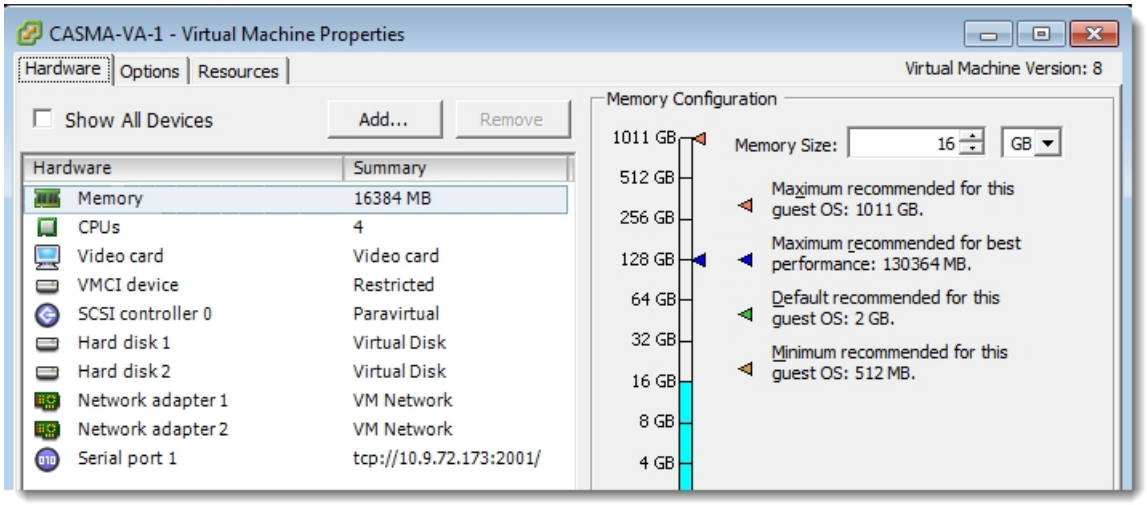
      If the VM is already powered off, the **Power > Power Off** option will be unavailable.

   b. Verify that the VM is powered off. Its icon should look similar to the following: 

4. Set the virtual memory size according to your VA model license. See "Table 2: Model-Specific Requirements" on page 9.

   a. Right-click the Content Analysis VM in your inventory list, and select **Edit Settings**. The Virtual Machine Properties dialog opens.

   b. In the **Hardware** tab, select **Memory**.



   c. For **Memory Size**, enter the value from the Virtual Memory column of "Table 2: Model-Specific Requirements" on page 9

   d. Click **OK**.

Power On the Virtual Appliance

1. Right-click the Content Analysis VM in your inventory list, and select **Power > Power On**.

2. Verify that the VM is powered on. Its icon should look similar to the following: 

Enter Your Serial Number

The first time you open the VM's console window, you will be prompted to enter the serial number of your Content Analysis virtual appliance; this process activates your virtual appliance. After your serial number is validated, you can set up the Content Analysis VA with the initial configuration wizard.

1. Locate the serial number that you retrieved earlier (see "Retrieve Your Serial Number" on page 14).
2. In the VMware client, click the Content Analysis VA (located in the inventory on the left).
3. Click the **Console** tab. The VMware client opens the Console window, where you are prompted to enter the serial number.
4. Type your serial number and press **Enter**.
5. If you receive an error message indicating that the serial number is not valid, check the number and try again.
   If the serial number is not accepted, stop and contact Symantec Support.
   When the system has determined the serial number is valid, the console will prompt you to press **Enter** three times.
6. Press **Enter** three times. The console displays a menu similar to the following.

```
Copyright (c) 2019, Symantec
Welcome to the Content Analysis CLI
Version: 2.4.1.1 Release id: 454010
--------------------MENU--------------------
1) Command Line Interface
2) Setup
----------------------------------------
Enter option:
```

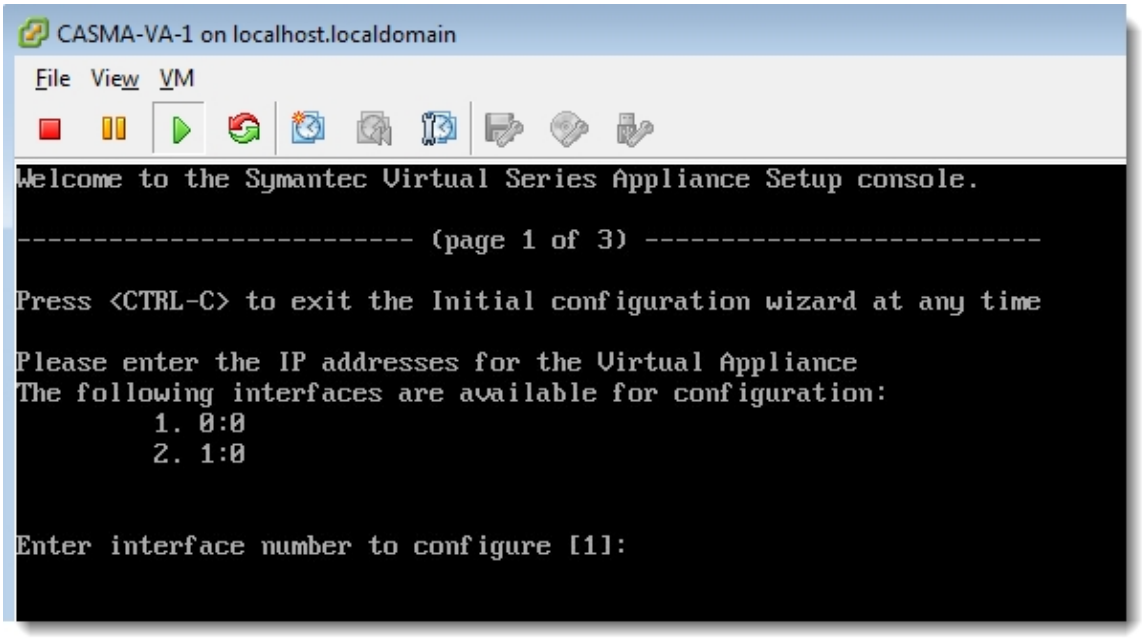
Configure the Virtual Appliance

Follow the prompts to complete initial configuration of Content Analysis.

> **Tip:** When you are typing in the Console window, the mouse is inactive and the cursor is restricted to the Console. To release the cursor from the Console and use the mouse elsewhere, press Ctrl+Alt. To return to typing in the Console, click the mouse anywhere in the Console window.

1. From the menu, select **2** to run the **Setup console** and start the initial configuration wizard.

   When prompted, hit any key to begin; the first page of the wizard opens.

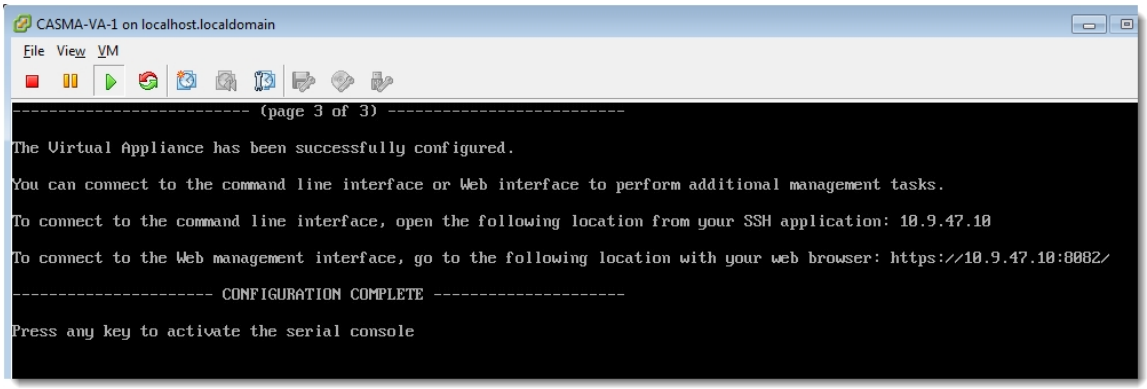


2. Select the number corresponding to the interface you want to configure; **1** (**0:0**, the management interface) is the default choice.
3. Referring to your notes in Prepare for Initial Configuration, enter the following details when prompted:
   - IP address (you will use this IP address for the web console)
   - Subnet mask
   - IP address for the default gateway
   - IP address for the primary DNS server

4. The wizard presents you with a summary of the interface settings and gives you an opportunity to change them. When the settings are correct, enter **N** at the **Would you like to change any of them?** prompt.
5. Create a console password for the admin user. It is recommended that the password be a combination of alphanumeric characters, at least 8 characters long.

> **Caution:** The console does not display the characters as you type them, nor are asterisk placeholders displayed.

6. Verify the console password by typing it again.
7. Enter an enable password; this password is required when using privileged mode in the command-line interface.
8. Verify the enable password by retyping it. The **Configuration Complete** message is displayed in the console.



Access the Web Management Console

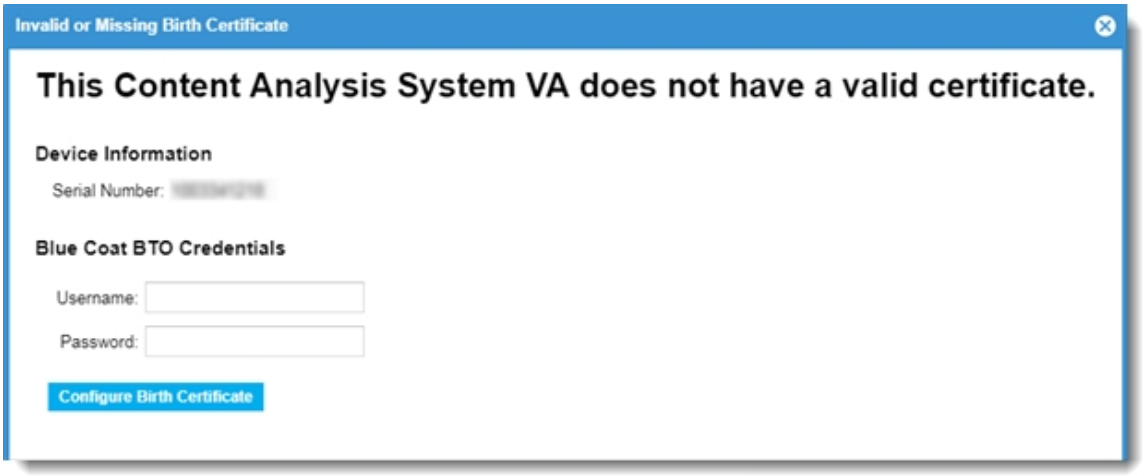
Verify that you can access the web management console. Refer to the *Release Notes* for a list of supported browsers.

1. Open a web browser.
2. In the address bar, enter the URL:
   `https://<IP_address>:8082 (where <IP_address> is the IP address you specified in the initial configuration wizard)`

   The web browser displays the Content Analysis login prompt.
3. Enter **admin** for the username, and enter the console password you configured during initial configuration.
4. When you initially log in to the web management console, you will be prompted to configure an appliance certificate for the VA. See "Install the VA Appliance Certificate and License" below.

Install the VA Appliance Certificate and License

The first time you log into the web management console, you are prompted to configure the virtual appliance certificate, which contains the virtual appliance base license.



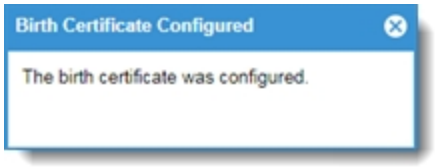
> **Note:** To install the appliance certificate, Content Analysis must be configured with the correct DNS server. The download will fail if Content Analysis cannot access the Internet or the DNS server.

1. Configure the appliance certificate:

    a. In the Invalid or Missing Birth Certificate dialog shown above, enter your MySymantec credentials.

    b. Click **Configure Birth Certificate**.

    The appliance certificate and base license are downloaded from Symantec and installed on the virtual appliance.



> **Tip:** If the configuration failed, make sure you have the correct DNS server configured on Content Analysis. To verify DNS settings, select **Settings > Network**, and make sure you can ping the DNS server from Content Analysis (**Utilities > Ping**).

2. Confirm that the license is active:

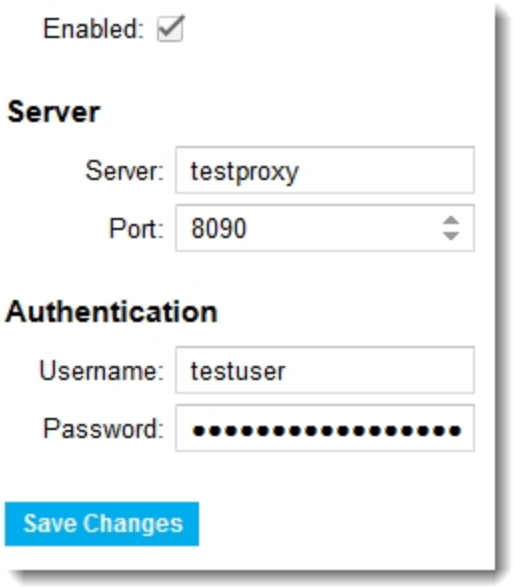
    a. Select **System > Licensing**.

    b. Verify that the base license has a check mark in the **Active** column.

Configure Explicit Proxy

If the secure environment your Content Analysisvirtual appliance is deployed in requires that all traffic destined for the Internet traverses a ProxySG appliance, you can configure the proxy settings in the Content Analysis management console.

1. Log in to the web console.
2. Browse to **Settings > Proxy.**



3. Click **Save Changes**.
4. Refresh the browser window.

Log onto the CLI

Log onto the CLI through an SSH connection or through the Content Analysis VMware console.

Log on using SSH

1. Open an SSH client (such as PuTTy) and specify the following information for a new host connection:
   - **Host Name (or IP address)**—The IP address that you specified for the Virtual Appliance
   - **Port**—22
2. Click **Open**.
3. The SSH window opens with a note about the private key.
4. Click **Yes** to accept the private key and dismiss the private key message. Future SSH connections to this virtual appliance will be compared against this key, and an alert will be presented if it does not match with the key saved during this initial session.
5. At the **login as:** prompt, type **admin** and press **Enter**.
6. At the **password:** prompt, enter your password and press **Enter**. The CLI prompt is displayed: **CAS>**.
7. To enter privileged mode, type **enable**, and enter the enable password when prompted.

Log on through the VMware Console

> **Note:** The VMware Console emulates an out-of-band console connection in that can be accessed regardless of the configured IP address for the VM.

1. In the VMware client, locate the Content Analysis VM in the inventory.
2. Click the **Console** tab, or right-click the Content Analysis Virtual Appliance, and select **Open Console**. The console prompts you to press Enter three times.
3. Press **Enter** three times. A menu displays in the Console window.
4. Enter **1** to use the Command Line Interface. The CLI prompt is displayed: **CAS>**.
5. To enter privileged mode, type **enable**, and enter the enable password when prompted.

Prevent Licensing Issues

To prevent licensing issues, ensure that the VA is allowed network access to the license validation server at **https://validation.es.bluecoat.com**.

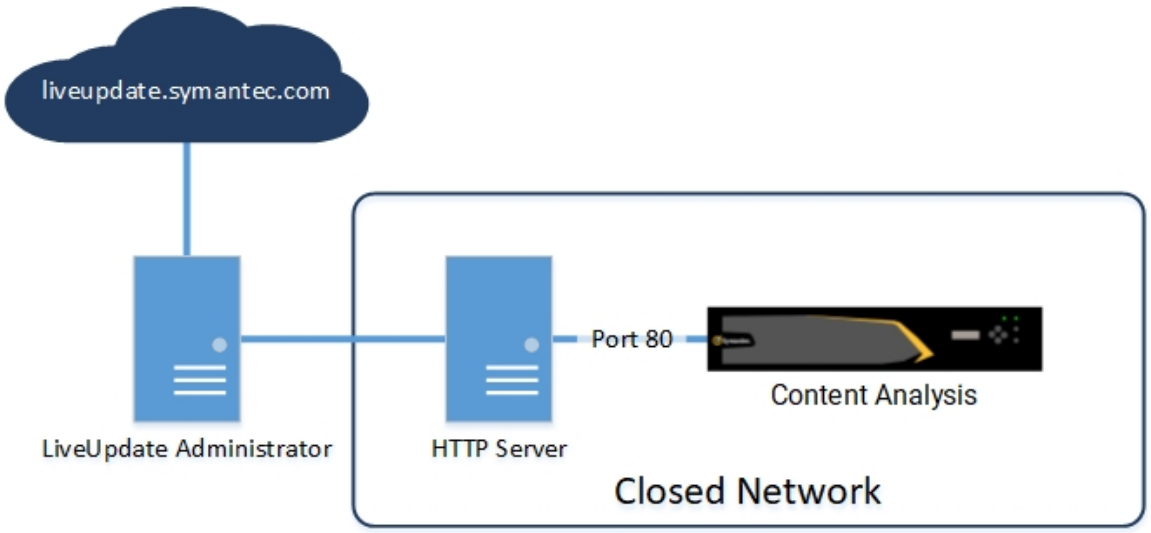
If communication with the server fails, a network issue may be present. A constant internet connection is required for Content Analysis to communicate regularly with the license validation server to confirm that the serial number is valid.

Duplicate Serial Numbers

If the license validation server detects duplicate serial numbers, your license is invalidated. Verify your license at the Symantec Licensing Portal (**licensing.symantec.com**) and contact Symantec Customer Care (np_customercare@symantec.com) if you have problems with your license or serial numbers.

Symantec Antivirus Updates in a Closed Network

If your Content Analysis appliance does not have access to the internet it cannot receive live updates for the Symantec antivirus engine. Use the Symantec LiveUpdate Administrator (LUA) to download and distribute Symantec AV pattern packages.



1. Go to the Symantec Support Center (**support.symantec.com**) and access the TECH134809 article.
2. Download the EXE file plus the *Getting Started Guide* and the *User's Guide*.
3. In the *Getting Started Guide* go to the "System Requirements for LiveUpdate Administrator" section to review supported servers, ports used, and installed components.

4. Install LUA on a server that can access **http://liveupdate.symantec.com/**. Consult the "Installing LiveUpdate Administrator" section in the *Getting Started Guide* for instructions.
5. In LUA, add Symantec Content Analysis as a product.
    a. Select **Configure > My Symantec Products** and click **Add New Products**.
    b. Select **Symantec Content Analysis** and click **OK**.
    c. Add a download schedule in the **Download and Distribute** tab or do a manual, one-time download for testing. Consult the "Scheduling Downloads" section of the *User's Guide* for instructions.
6. Add the Symantec update server as the default distribution center.
    a. Select **Configure > Distribution Center**.
    b. Select **Default Production Distribution Center** and click **Edit**.
    c. In the *Product List* section click **Add**.
    d. Select **Symantec Content Analysis <*version*> English** and click **OK**.
    e. Add a distribution schedule in the **Download and Distribute** tab or do a manual, one-time download for testing. Consult the "Scheduling Distribution" section of the *User's Guide* for instructions.
7. Create an HTTP server that Content Analysis can access, listening on port 80.
8. Host the files in **C:\Program Files (x86)\Symantec\LiveUpdate Administrator\clu-prod** in the web-root directory of the HTTP server that you just created. You can schedule distribution of files to this directory if you add the server as a distribution center on the **Download and Distribute** tab.

    > **Note:** The directory path could be different if you used a different directory during LUA installation.

9. Perform one of these options to direct Content Analysis to your HTTP server for updates:
    - Create an entry on your local DNS server to add **liveupdate.symantec.com** as the IP address of your HTTP server. By default Content Analysis tries to find the latest updates at that address.
    - Go to **Services > AV Scanning Behavior > Symantec Options** and input the URL of the HTTP server for **Live Update**.