Telestream

Security Guide

Release: 9.0

Revision: 1.0

November 3, 2023

Copyrights and Trademark Notices

Contents

Telestream Contact Information

To obtain product information, technical support, or provide comments on this guide, contact us using our web site, email, or phone number as listed below.

Resource	Contact Information
Content Conductor Technical Support	Web Site: https://www.telestream.net/telestream-support/content-conductor/support.htm Depending on the problem severity, we will respond to your request within 24 business hours. For P1, we will respond within 1 hour. Please see the Maintenance & Support Guide for these definitions. • Support hours for customers are Monday-Friday, 7am-6pm local time. • P1 issues for customers are 24/7.
Telestream, LLC	Web Site: www.telestream.net Sales and Marketing Email: info@telestream.net Telestream, LLC 848 Gold Flat Road, Suite 1 Nevada City, CA USA 95959
International Distributor Support	Web Site: www.telestream.net See the Telestream Web site for your regional authorized Telestream distributor.
Telestream Technical Writers	Email: techwriter@telestream.net Share comments about this or other Telestream documents.

Preface

This book describes the requirements for a secure Content Conductor installation. The manual assumes a working knowledge of the Windows operating system and additional Content Conductor related concepts.

Audience

This document is intended for the Installation Team, System Administrators, and Users.

Documentation Accessibility

For information about our commitment to accessibility, visit the Support Portal located at https://www.telestream.net/telestream-support/.

Related Documents

For more information see the Content Conductor library located at:

https://www.telestream.net/telestream-support/content-conductor/support.htm

Document Updates

The following table identifies updates made to this document.

Date	Update
October 2022	Created book for 9.0 release.
March 2023	Updated document from DIVA Core to Content Manager.
June 2023	Updated book for 9.0 release.
September 2023	Change Content Manager > Content Conductor. Publish version 9.0 PDF.

Overview

The general principles of Content Conductor application security should be adhered to for a secure system. See the Port Utilization section in the Content Conductor Installation and Configuration Guide for detailed port requirements and the Content Conductor Architecture, Concepts and Glossary book for a general understanding of Content Conductor system components and a centralized glossary of terms used within Content Conductor.

Topics

Keep Software up to Date

Stay current with the version of Content Conductor that is being run. Current versions of the software are available for download at the Software Delivery Cloud located at:

https://www.telestream.net/telestream-support/content-manager/support.htm

Restrict Network Access to Critical Services

Content Conductor uses an identified list of TCP and UDP ports, as well as HTTPS access for REST APIs. For Content Conductor to operate correctly, these ports may have to have access restricted, or permission granted, on a per server basis. Refer to Content Conductor Installation Guide Port Utilization for the detailed list of ports used.

Run as Content Conductor User and use Principle of Least Privilege Where Possible

Do not run Content Conductor services using an Administrator (or root) operating system user account. Always run all Content Conductor services using a dedicated operating system user named diva.

Content Conductor User Profiles in the Web App

The web app has replaced the legacy control panel and configuration utility. User profiles are configured by navigating to the Configuration > User Management page on the left menu of the web app. Refer to the Content Conductor Installation and Configuration Guide for details on user accounts and permissions.

The Content Conductor system provides five fixed user profiles as follows:

- System Administrator
- Administrator
- Advanced Operator
- User
- Service

All accounts require a password to obtain access. Passwords must be assigned in the web app before using these profiles.

Passwords are created during installation and configuration for both the Administrator and Operator accounts. Telestream recommends that the passwords be changed every 180 days (minimum) thereafter. Passwords must be made available for Technical Support if needed.

Note: Each Content Conductor component uses its own dedicated user name and password to connect to the main application.

Postgres Database Security

Access rules are defined in Postgres configuration to control and restrict access to the Content Conductor database. Changes to those settings should be made carefully to not jeopardize database access restrictions.

Monitor System Activity

Monitor system activity to determine how well Content Conductor is operating and whether it is logging any unusual activity. Check the log files located in the installation directory under /Program/log/. Refer to the Content Conductor Operations Guide for details on system monitoring and logs.

Keep up to Date on Latest Security Information

For security information and alerts for a large variety of software products, see http://www.us-cert.gov.

The primary way to keep up to date on security matters is to run the most current release of the Content Conductor software.

Using Anti-virus Software

Install Anti-virus and exclude the Content Conductor processes and storage (for performance reasons).

Installation

This section outlines the planning process for a secure installation and describes several recommended deployment topologies for the systems.

Topics

Understanding the Environment

To better understand security needs, the following questions must be asked:

Which Resources Need to be Protected?

Many of the resources in the production environment can be protected. Consider the type of resources that to protect when determining the level of security to provide.

Protect the following resources when using Content Conductor:

Primary Data Disks and Disk Arrays

There are Data Disk and Cache Disk resources used to build Content Conductor systems. They are typically local or remote disks connected to the Content Conductor systems. Independent access to these disks (other than by Content Conductor) presents a security risk. This type of external access might be from a rogue system that reads or writes to these disks, or from an internal system that accidentally provides access to these disk devices.

Database Disk, Metadata Disk, and Backup Disks

There are Database Disk, Metadata Disk and Backup Disk resources used to build Content Conductor systems with complex objects. They are typically local or remote disks connected to the Content Conductor systems. Independent access to these disks (other than by Content Conductor) presents a security risk. This type of external access might be from a rogue system that reads or writes to these disks, or from an internal system that accidentally provides access to these disk devices.

Tapes and Tape Groups

It is a security risk to allow independent access to tapes where data is written; typically in a tape library controlled by Content Conductor systems.

Export Tape Metadata

Tape Metadata dumps that are created from export operations contain data and metadata. This data and metadata permissions must be restricted to only the Administrator (or root) operating system account, or the Content Conductor operating system user (or Tape Group) during a routine export or import activity.

Configuration Files and Settings

Content Conductor system configuration settings must be protected from operating system level non-administrator users. Making the configuration files writable to non-administrative operating system users presents a security risk, therefore, these file permissions must be restricted to only the Administrator (or root) operating system account, or the Content Conductor operating system user.

From whom are the resources being protected?

In general, the resources described in the previous sections must be protected from all non-administrator access on a configured system, or from a rogue external system that can access these resources through the WAN or FC Fabric.

What will happen if the protections on strategic resources fails?

Protection failures against strategic resources can range from inappropriate access (that is, access to data outside of normal operations) to data corruption (writing to disk or tape outside of normal permissions).

Recommended Deployment Topologies

This section focuses on security concerns. Consider the following points when installing and configuring Content Conductor, and refer to the Content Conductor Installation and Configuration Guide for details.

Separate Metadata Network

For connections between Content Conductor services components, connection to the Metadata Database, and the connection from its clients, provide a separate TCP/IP network and switch hardware that is not connected to any WAN. Because the metadata traffic is implemented using TCP/IP, an external attack on this traffic is theoretically possible. Configuring a separate metadata network mitigates this risk and also provides enhanced performance. If a separate network is infeasible, at least deny traffic to the Content Conductor ports from the external WAN and any untrusted hosts on the network. See *Restrict Network Access to Critical Services*.

Fiber Channel Zoning

Use Fiber Channel Zoning to deny access to the Content Conductor disks connected through the Fiber Channel from any server that does not require access to the disks. Preferably, use a separate FC switch to physically connect only to the servers that require access.

Safeguard SAN Disks Configuration Access

SAN RAID disks can usually be accessed for administrative purposes through TCP/IP or more typically HTTP. Protect the disks from external access by limiting the administrative access to SAN RAID disks to systems only within a trusted domain. Also, change the default password on the disk arrays.

Install the Content Conductor Package

First, install only required Content Conductor services for the environment. For example, if not planning to run the web app from a system, then deselect them in the list of components to be installed during installation. The default Content Conductor installation directory permissions and owners must be restricted to only the Administrator (or root) account, or the Content Conductor operating system user. Refer to the Content Conductor Installation and Configuration Guide for full installation details.

Tape Security

Prevent external access to tapes inside a tape library controlled by the Content Conductor system. Unauthorized access to tapes can compromise or destroy user data.

Backup Production Databases

Set up and perform database backups using the Content Conductor Backup Service. Permissions for the backup dump must be restricted to only the Administrator (or root) operating system account, or the Content Conductor operating system user. Telestream recommends configuring a minimum of one (ideally two) remote database backup location other than the primary one located on the Manager primary location.

Refer to the Content Conductor Database and BKS Installation, Configuration and Operations Guide for details.

Post-Installation Configuration

After installing any of the Content Conductor components, go through the security checklist in *Secure Deployment Checklist*.

Security Features

To avoid potential security threats, customers operating Content Conductor must be concerned about authentication and authorization of the system. These security threats can be minimized by proper configuration and by following the post-installation checklist in *Secure Deployment Checklist*.

Topics

The Security Model

The critical security features that provide protections against security threats are:

Authentication

Ensures that only authorized individuals are granted access to the system and data.

Authorization

Access control to system privileges and data. This feature builds on authentication to ensure that individuals get only appropriate access.

Tape Group Encryption

Tape drive encryption securely supports bulk tape migration between Content Conductor systems.

SSL Authentication and Secure Communications

Content Conductor includes SSL Authentication for services, and to secure Content Conductor internal and API communications. Certificate authentication provides unique identification and secure communication for each Content Conductor Service in a network.

web app Access Control

Access control in Content Conductor is divided into six profiles as described below. Accounts require a password to obtain access. Account passwords must be assigned in the web app before using these profiles.

System Administrator (sysadmin)

The System Administrator uses the sysadmin profile to log into the web app. This profile allows access to all functions of the web app and should only be used by System Administrator when making additions, deletion, or changes to the Content Conductor system.

Administrator (admin)

To issue requests to Content Conductor, such as archive or restore requests, or to eject a tape from a library, the Administrator profile must be used. The password for this profile must be assigned in the web app before using the profile. For more information, refer to the Content Conductor Installation and Configuration Guide on the Content Conductor Technical Support site.

Advanced Operator (*advoperator*)

In addition to User profile permissions, the Advanced Operator profile in the web app can now optionally enable privileges for canceling and changing the priority of requests. The options are defined in the web app. By default, this option is disabled.

Operator (operator)

In addition to User profile permissions, the Operator profile in the web app can now optionally enable privileges for canceling and changing the priority of requests. The options are defined in the web app. By default, this option is disabled.

User (user)

This is a very restrictive profile. After the connection to the Manager is established, the web app will only allow the user to monitor Content Conductor operations. This is known as the User profile. Not all functions that issue commands to Content Conductor are accessible while in the User profile mode, enabling situations where monitoring is required but no commands are permitted to be sent to Content Conductor.

Tape Group Encryption

This release includes tape drive encryption that securely supports bulk tape migration between Content Conductor systems.

After enabling encryption on a tape group, all additional tapes added to the group will also be encrypted. However, any existing tapes in the group remain unencrypted if encryption was previously disabled.

Enabling encryption on a tape group generates an encryption key, which is also encrypted. The encryption key can be changed at any time. New tapes added to the group after the change will use the new encryption key. The existing tapes that were already encrypted will continue to use the original key. Therefore, tapes in the same tape group can have different encryption keys. The Manager must be notified of the change when updating the encryption key.

Disabling encryption (after it is already enabled) only affects additional tapes added to the group, and the existing tapes remain encrypted.

S3 Server-side Encryption

These options can be added to the Storage options field in order to configure S3 server-side encryption.

Option Syntax	Description
`-server_side_encryption=<KMS or AES256>`	This option must be set in order to enable S3 server-side encryption. Content Conductor supports SSE-S3, SSE-OSS and KSM. Set this option to AES256 if using SSE-S3 or SSE-OSS. Set this option to KMS if using KMS is required.
`-kms_key_id=<kms key ID>`	If `-sse` is set to KMS, this option can be set if Content Conductor should use a specific encryption key identified by its key id. This option is supported by aws:s3 and alibaba:oss.
`-bucket_key_enabled` (aws:s3 specific)	If `-sse` is set to KMS, `-bucket-key-enabled` can be set if the kms key id to be used is associated with the bucket. This option is supported by aws:s3 but not alibaba:oss. With Alibaba, there is no need to configure server side encryption on the Content Conductor side if the bucket is configured with a default server-side encryption.

Note: The `-kms-key-id` and `-bucket-key-enabled` parameters are mutually exclusive. If both are specified by mistake, Content Conductor will use `-kms-key-id` and ignore `-bucket-key-enabled`.

Manager-Actor Communications

The options previously described are converted by the Manager into new elements of the transfer request message.

Example:

```
<TransferRequest ...>
...
<DiskPath><https://s3.amazonaws.com</DiskPath>>
<Proxy></Proxy>
<Login></Login>
<Password></Password>
<ServiceName>S3</ServiceName>
<IdentityDomain>us-east-1</IdentityDomain>
<ThreadsPerTransfer>5</ThreadsPerTransfer>
<PartSize>5</PartSize>
<DisableETagVerification>false</DisableETagVerification>
<ContainerName>diva-b6e27aae40abf4f8f04d755d18fdb82c256de0d6-
00000000</ContainerName>
<StorageClass>STANDARD</StorageClass>
<VirtualHostedStyle>false</VirtualHostedStyle>
<ServerSideEncryption>kms</ServerSideEncryption>
<KmsKeyId>1234abcd-12ab-34cd-56ef-1234567890ab</KmsKeyId>
<BucketKeyEnabled>true</BucketKeyEnabled>
<AccountName>AWS_STD_172.16.10.192_12E76933EF49</AccountName>
<StorageOptions>-storage_class STANDARD -storage_location S3 -
restore_tier NONE -virtual_hosted_style false -
disable_etag_verification false -server_side_encryption AES256 -
aws_kms_key_id true -bucket_key_enabled true</StorageOptions>
</DeviceDisk>
...
</TransferRequest>
```

Enforce SSE-S3 or SSE-KMS at Bucket Level

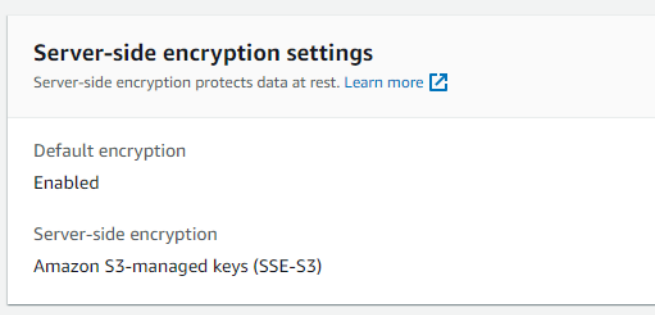
When using SSE, the SSE option must be set to AES256 or aws:kms. It is recommended to add a bucket policy to prevent uploads without valid encryption headers.

When there is a bucket policy preventing uploads without encryption, or bad encryption header, the S3 server returns an HTTP error 403. Here is the error message returned by the Core Actor when it happens:

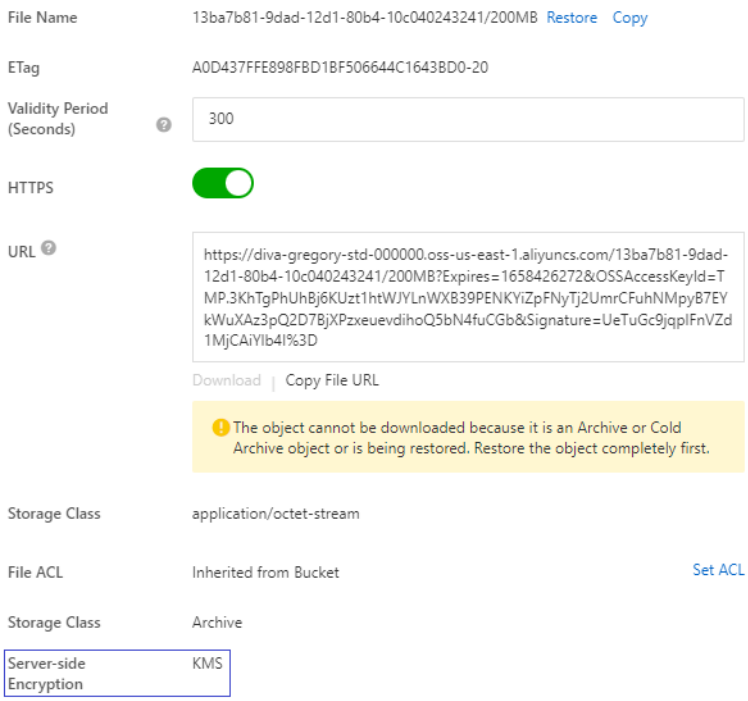
```
Error during disk instance closure divastorage_GREG_STD_000002
[StorageCloudAPI error [16ba7b81-9dad-12d1-80b4-10c040243241.axf
upload failed, http response code: 403 [AccessDenied: Access
Denied]]]
```

Checking if the Files are Encrypted

With AWS S3 this information is visible as shown here:

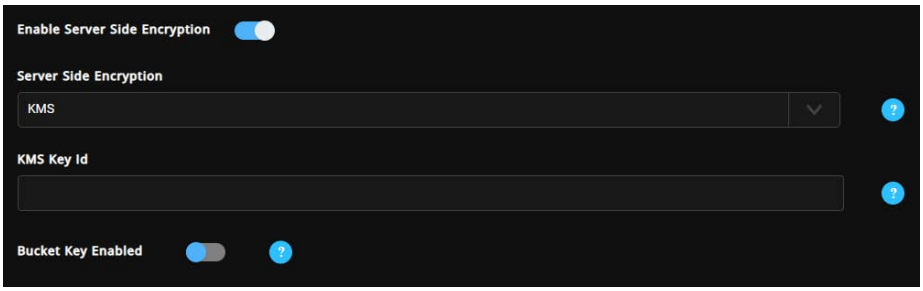


Similar information is available with Alibaba OSS in the detail view of a particular file as shown here:



Web App Support

SSE for S3 buckets can be enabled in the web app Configuration page. Enable Server Side Encryption only displays for S3 Cloud Buckets. If enabled, Server Side Encryption, KMS Key Id, and Bucket Key Enabled display:



Server-side Encryption

Secure Sockets Layer and Authentication

Content Conductor includes SSL Certificate Authentication for authentication of services, and securing the internal and API communications in Content Conductor. Certificate authentication provides unique identification and secure communications for each Content Conductor service in a network.

Content Conductor includes a Default Root CA (Certificate Authority) called DIVA_CA. The DIVA_CA Certificate Authority is a self-signed authority that signs all SSL certificates for the Content Conductor Core services. Every Content Conductor service now has its own password protected private key and a SSL certificate signed by the DIVA_CA authority.

Certificate authentication functions similar to identification cards like passports and drivers licenses. For example, passports and drivers licenses are issued by recognized government authorities. SSL certificates are signed by a recognized CA. An SSL certificate verifies the identity of its owner. When the SSL certificate is presented to others, it helps verify the identity of its owner based on the quality of the contents of the certificate.

An external third party CA (for example, VeriSign and Comodo) can be used to generate and sign the certificates.

External Certificate Authorities

External third party CAs (for example, VeriSign, Comodo, and so on) are usable with Content Conductor. The external CA must create a CSR (Certificate Signing Request) for DIVA_CA, signed by the third party CA, and the third party certificate must be added to the Trust Store to satisfy the SSL Certificate Chain.

When connecting to the web app for the first time, there is usually a security error page displayed by the web browser. This error means that the HTTPS server certificate is not trusted by the browser. This is the certificate for the REST API Gateway (*DIVA\Program\security\certificates\RestAPIService.p12*). This issue is caused by the fact that the certificates generated by Content Conductor were self-signed. This is verifiable by showing the certificate because it has been issued "by" and "to" the same organization. You may accept the risk and continue to connect, but you will always get the same error for every new connection.

The Content Conductor security tool (*DIVA\Program\security\bin\DIVASecurityTool.bat*) has been fixed to generate certificates signed DIVA certificate authority (DIVA_CA). With the new security tool, the new certificates are no longer self-signed.

Before applying the security tool (before Content Conductor 9.0), make sure to make a backup copy of *DIVA\Program\DIVA_CA\DIVA_CA.cnf* because it contains the list of domains or IP addresses to connect to the web app. If the web app is being accessed using `https://IP_Address/DIVAWebUI/login`, the IP address must be listed in the alt_names section. This also applies to domain names or host names. The second security tool option will automatically add the IP address and the host name of the server to the alt_names section is at the end of the file.

With the fixed security tool, you must generate new certificates (option 2) and restart all the Content Conductor services. Contact Telestream Technical Support for assistance as necessary.

Security Tools

Content Conductor release includes *DivaSecurityTool.bat*, a Windows security tool.

The tool is located in the %TSCM_HOME%/security/bin directory. You can use it to generate SSL certificates used for secure communication in Content Conductor.

Content Conductor API Security Changes

The Content Conductor REST API includes the ability to establish secure communications with the Manager. Telestream recommends using the REST API rather than the previous existing APIs (that is, DIVA Enterprise Connect, DIVAS, Java and C++). The REST API offers new and enhanced features and is integrated into the Content Conductor and required by the web app to function.

Dual Ports

All internal Content Conductor services can only connect to secure ports. The web app will report an SSL Handshake Timeout if attempting to connect to the non-secure port.

SSL and Authentication

Content Conductor consist of services in Java and C++. The format in how certificates and keys are represented are different in each. Content Conductor has the keys and

certificates for JAVA services in a Java Keystore file, and in PEM (Privacy Enhanced Mail) format files for the C++ services.

The Manager can simultaneously support two communications ports—one secure, and one unsecure. The default secure port number is 8000 and the unsecure default port number is 9000.

All internal Content Conductor Core 8.x services (web app, Migration Utility, Actor, SPM, WFM, SNMP, Robot Manager, RDTU, and Migration Services) can only connect to secure ports. The web app will report an SSL Handshake Timeout if attempting to connect to the non-secure port. Clients using the Java or C++ API are allowed to connect to either port.

The following is a relative snippet from the Manager configuration file:

```
# Port number on which the DIVA Manager is waiting for incoming
connections.
# Note: If you are using a Sony library and plan to execute the
DIVA Manager
# on the same machine as the PetaSite Controller (PSC) software, be
aware
# that the PSC server uses the 9000 port and that this cannot be
modified.
# In that situation, you have to use a different port for the DIVA
Manager.
# This same warning applies to FlipFactory which uses ports 9000
and 9001.
# The default value is 9000.
DIVAMANAGER_PORT=9000

# Secure port number on which the DIVA Manager is waiting for
incoming connections.
# The default value is 8000.
DIVAMANAGER_SECURE_PORT=8000
```

A new folder called %TSCM_API_HOME%/security is added to the Content Conductor API installation structure as follows:

```
%TSCM_API_HOME%
 security
  conf
```

The conf folder contains the SSLSettings.conf file that is used to configure the SSL handshake timeout.

Secure Communication with the Database

Secure Deployment Checklist

1. Set strong passwords for Administrator (or root) and any other operating system accounts that have any Content Conductor administrator or service roles assigned to them, including:
   - Postgres User IDs (if being used)
   - Any disk array administrative accounts.
2. Do not use a Local Administrator operating system account. Assign roles as needed to other user accounts.
3. Change the default password for the sysadmin user. Upon installation the default is `changeit`.
4. Set a strong password for Administrator and Operator for the Web App. A password must be assigned for these profiles in the Web App before use.
5. Set a strong password for the database login.
6. Install a firewall on every system and apply the default Content Conductor port rules. Restrict access to the Content Conductor API (TCP/9000) to IP addresses that require access using firewall rules.
7. Install operating system and Content Conductor updates on a periodic basis since they include security updates.
8. Install Anti-virus and exclude the Content Conductor processes and storage (for performance reasons).
9. It is best practice to segregate FC disks and FC tape drives either physically or through FC Zoning so that disks and tape devices do not share the same HBA port. For managed disks, only Actors should have access to disk and the tape drives. This security practice helps prevent loss-of-data accidents resulting from accidental overwriting of tape or disk.
10. Set up an appropriate set of backups of the Content Conductor configuration and database. Backups are part of security and provide a way of restoring data lost either accidentally, or through some type of breach. Backups should include some policy while being transported to an off-site location. Backups need to be protected to the same degree as tape groups and disk.
11. Technical Support strongly recommends using an external Certificate Authority for additional security.