DIVA Connect

Security Guide

Release 3.1.0

Version 1.0

December 2021

telestream | DIVA

Copyrights and Trademark Notices

Specifications subject to change without notice. Copyright © 2021 Telestream, LLC and its Affiliates. Telestream, CaptionMaker, Cerify, DIVA, Episode, Flip4Mac, FlipFactory, Flip Player, Gameshow, GraphicsFactory, Kumulate, Lightspeed, MetaFlip, Post Producer, Prism, ScreenFlow, Split-and-Stitch, Switch, Tempo, TrafficManager, Vantage, VOD Producer, and Wirecast are registered trademarks and Aurora, ContentAgent, Cricket, e-Captioning, Inspector, iQ, iVMS, iVMS ASM, MacCaption, Pipeline, Sentry, Surveyor, Vantage Cloud Port, CaptureVU, Cerify, FlexVU, PRISM, Sentry, Stay Genlock, Aurora, and Vidchecker are trademarks of Telestream, LLC and its Affiliates. All other trademarks are the property of their respective owners.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

Contents

3 Security Features

A Secure Deployment Checklist

Preface

DIVA Connect Security Guide includes information about the DIVA Connect product and explains the general principles of application security.

Audience

This guide is intended for anyone involved with using security features and secure installation and configuration of DIVA Connect.

Documentation Accessibility

For information about Telestream's commitment to accessibility, visit the Telestream Support Portal located at https://www.telestream.net/telestream-support/diva/support.htm.

Access to Telestream Support

Telestream customers that have purchased support have access to electronic support through the Telestream Support Portal located at https://www.telestream.net/telestream-support/diva/support.htm.

Document Updates

The following table identifies updates made to this document.

Date	Update
February 2021	Rebranded document to Telestream
	Updated copyright notices
July 2021	Updated book details for release 3.0.0
December 2021	Updated release date and release number; no other changes.

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.

Convention	Meaning
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
monospace	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.
blue text	Blue text indicates a link to an outside source, or to another chapter, section, or glossary term in this book.

1

Overview

This chapter provides an overview of the DIVA Connect 3.1.0 product and explains the general principles of application security.

Product Overview

DIVA Connect provides a unified view of archived content across multiple, distributed DIVA Core systems. DIVA Core is a scalable content storage management system supporting archival to tape libraries and disk systems. DIVA Connect facilitates the moving of content back and forth among DIVA Core sites, and from customer Source and Destination Servers and disks. It performs its tasks for the purposes of disaster recovery, content distribution, access control, performance, and content availability.

DIVA Connect consists of the following major components:

DIVA Connect ClientAdapter Service

Application clients that want to use the DIVA Core API, or want to use the DIVA Connect GUI, connect to the DIVA Connect ClientAdapter Service. This DIVA Connect service accepts web and socket connections from applications and processes the requests. A ClientAdapter is configured on each site that has applications that are local to the site where DIVA Core and DIVA Connect are installed.

DIVA Connect ManagerAdapter Service

The DIVA Connect ManagerAdapter Service serves as a bridge between DIVA Connect and the DIVA Core Manager. It must be configured to provide remote access by other DIVA Connect systems.

DIVA Connect DbSync Service

The DIVA Connect DbSync Service is responsible for synchronizing asset information from multiple DIVA Core sites, and storing the information in the DIVA Connect database. DbSync communicates remotely with ManagerAdapter services on multiple sites to synchronize archived object information. DbSync is typically deployed with the ClientAdapter. The DbSync service and ClientAdapter both require direct access to the DIVA Connect database.

DIVA Connect User Interface (*DIVA ConnectUI*)

DIVA ConnectUI is a GUI application that enables monitoring DIVA Connect requests, and view, copy, and delete DIVA Connect assets (*DIVA archived objects*) across multiple DIVA Core sites. All DIVA Connect level requests can be monitored, whether issued through the API or through the UI itself. You can also view asset information for all configured DIVA Core sites, regardless

of whether the asset was archived through DIVA Connect. DIVA ConnectUI provides flexible ways of querying both request information and asset information.

General Security Principles

The following sections describe the fundamental principles that are required to use any application securely.

Keep Software up to Date

Stay current with the version of DIVA Connect that you run. You can find current versions of the software for download at the Telestream website located at

https://www.telestream.net/telestream-support/diva/support.htm

Restrict Network Access to Critical Services

DIVA Connect uses the following TCP/IP ports by default:

- tcp/9801 is the default WebService port used by the DIVA Connect ClientAdapter
- tcp/7101 is the default API socket port used by DIVA Connect ClientAdapter (*you can configure other ports*)
- tcp/9800 is the default WebService port used by the DIVA Connect ManagerAdapter

> **Note:** Not all of these ports must be exposed externally, and are based on configuration and usage.

The DbSync port (*by default, port 9802*) should remain blocked for network access outside of the server machine running DIVA Connect.

Use Principle of Least Privilege where Possible

DIVA Connect services should not be run as admin or root. Running the services using a different operating system user (*than the user used to administer the application*) contributes to overall system security.

The DIVA Connect Linux installer requires two users to complete DIVA Connect installation - diva and an operating system user. Administrators and Operators use the diva account to install and monitor DIVA Connect. The operating system user controls the DIVA Connect services.

Firewalls must restrict ports to only those that are required. DIVA Connect contains access control features (*briefly described in* Access Control) used to restrict users and systems to the least privilege possible.

Monitor System Activity

You must monitor system activity to determine how well DIVA Connect is operating and whether it is logging any unusual activity. Check the log files located in the $DIVA Connect_HOME/Program/log folder.

Keep Up To Date on Latest Security Information

You can access several sources of security information and alerts for a large variety of software products at:

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 DIVA Connect software.

2

Secure Installation

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

Understand Your Environment

To better understand security needs, ask the following questions:

Which resources need to be protected?

You can protect many of the resources in the production environment. Consider the type of resources to protect when determining the level of security to provide.

When using DIVA Connect, you must protect the following resources:

DIVA Connect Servers

DIVA Connect is installed on a server attached to one or more disks (*either a local or remote disk directly connected to the DIVA Connect system*). Independent access to these disks (*not through DIVA Connect*) 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

There are database software and data resources used to build DIVA Connect systems. The data exists typically on local or remote disks connected to the DIVA Connect systems. Independent access to these disks (*not through DIVA Connect*) 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.

DIVA Core Servers and Archive Media

DIVA Connect uses DIVA Core Source and Destination Servers, and DIVA archival systems (*disk or tape*) in the process of satisfying its requests. Unwarranted independent access to these server disks and system medium, which are typically controlled by DIVA Core systems, is a security risk. The Servers that are used as temporary data stores for DIVA Connect copy operations, should have restricted access, and you should consider dedicating these Servers solely to DIVA Connect operations - and also ensure that the transfers are encrypted or initiated over a trusted network.

Configuration Files and Settings

DIVA Connect system configuration settings must be protected from operating system level non-administrator users. In general, these settings are protected automatically by operating

system level administrative users. Making the configuration files writable to non-administrative operating system users presents a security risk.

From whom are the resources being protected?

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

What will happen if the protections on strategic resources fail?

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

Recommended Deployment Technologies

This section describes installation and configuration of a secure infrastructure component.

For information about installing DIVA Connect, refer to the DIVA Connect Installation, Configuration, and Operations Guide in the DIVA Core Documentation library at:

https://www.telestream.net/telestream-support/diva/support.htm

Consider the following points when installing and configuring DIVA Connect.

DIVA Connect Installation

You should install only those DIVA Connect components that you require. For example, if you plan to run only DIVA ConnectUI from a client computer, deselect the **DIVA Connect Services** check box in the list of components to be installed during installation. The default DIVA Connect installation directory permissions and owners should not be changed after installation without considering the security implications of such changes.

Connecting to DIVA Core

Telestream recommends that you install the ManagerAdapter component on the DIVA Core Manager system for increased system security. If external access to the DIVA Core Manager port is not needed, it is recommended to block the port using firewall software. In addition, it will often not be necessary to allow external network access to the DIVA Connect DbSync WebService port.

If you connect to a remote DIVA Core instance over a WAN, ensure that you connect over a trusted network. Also, consider connecting to the site using SSL/TLS to the remote site's ManagerAdapter port.

Safeguard Disk Systems

Use FC Zoning to deny access to the DIVA Connect disks connected through Fibre 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 requiring access.

SAN RAID disks can usually be accessed for administrative purposes through TCP/IP or more typically HTTP. You must 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.

Post-installation Configuration

After installing any portion of DIVA Connect, go through the Security Checklist in Appendix A.

3

Security Features

To avoid potential security threats, customers operating DIVA Connect must be concerned about authentication and authorization of the system.

These security threats can be minimized by proper configuration and by following the postinstallation checklist in Appendix A.

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.

Authentication

DIVA Connect services can perform authentication using several methods:

- **SSL / TLS Certificates** - DIVA Connect consults a certificate truststore when DIVA Connect creates an outbound connection to a remote DIVA Connect service. This helps to insure that DIVA Connect is connecting to genuine DIVA Connect services. To create a secure connection from the DIVA Connect ClientAdapter to a ManagerAdapter instance, you must connect through the ManagerAdapter using a `ConnectionType` identified as **WebServices**.
- **Access Rules** - While technically a form of access control, access rules can filter inbound connections based on the inbound IP address. This feature is necessary to help insure that only approved systems have appropriate access to DIVA Connect services.

> **Caution:** DIVA Connect services use database passwords as part of their configuration. Passwords must be changed immediately after installation and every 180 days (*minimum*) thereafter. After the change has been made, you must store the passwords in a safe location, offline, where they can be made available for Technical Support if needed.

- **User Login** - Consider configuring a user login for DIVA Connect UI, especially when accessing the UI from remote networks. To do this, use DIVA ConnectAdmin to create a username and password. Set the ClientAdapter parameter `UserAuthEnabled` to `true`. Then,

configure DIVA Connect UI to prompt for a username/password by setting the parameter userlogin to true in the divaconnectui.properties file.

- **Database Password** - Consider using the DIVA ConnectAdmin option to encrypt the database password, especially if the database is remote or shared with other systems. Follow the instructions in DIVA ConnectAdmin to update the DIVA Connect configuration files.

Access Control

Access rules can be created to limit the operations that certain users or systems may perform in the distributed archive system. Access rules can be run in the following ways:

- **ClientAdapter /MultiDiva Mode** - Restricts the types of DIVA Connect requests that can be executed.
- **ManagerAdapter** - Restricts the types of DIVA Core requests that can be executed to satisfy a DIVA Connect request (*possibly requested by a remote system*).

Access rules can affect requests initiated from the DIVA ConnectUI or from an API socket connection (*possibly initiated by a MAM or automation system*).

A DIVA Connect request can have access rules executed on it at the DIVA Connect level or at the DIVA Core level. At the DIVA Connect level, the ClientAdapter processes the request where the request was received. At the DIVA Core level, a remote ManagerAdapter processes DIVA Core requests issued to satisfy the DIVA Connect request.

Telestream recommends you create the most restrictive set of rules that meet your application requirements. For example, if only administrators need to perform global deletes, insure that others are denied access to that functionality. If a group of system users only require access to a finite list of Source and Destination Servers, insure that those users can issue requests against only those specific Servers.

Also consider the sites used to satisfy requests. For example, if users on the local site have no reason to perform copies where neither the source nor target sites are the local site (*this is possible using DIVA Connect*), configure these rules in the ClientAdapter configuration.

Finally, consider specific constructs in requests you want to exclude across the board. For example, if you do not need to address objects with only the Object Name (*without the category*), then exclude all requests having blank categories.

Additionally, each ClientAdapter WorkflowProfile contains the list of valid messages that can be processed by requests assigned to the WorkflowProfile. In **MultiDiva Mode**, this provides a way of excluding specific messages from processing (*including informational messages*).

Telestream recommends starting with the default rules defined in the AccessRules.xml.ini file even if you do not define your own access rules. For more information on DIVA Connect Access Control features, refer to the *DIVA Connect Installation, Configuration, and Operations Guide* located at https://www.telestream.net/telestream-support/diva/support.htm.

Configuring SSL/TLS

You can use SSL in the following components:

- In the ClientAdapter, for web/UI connections. To enable, set the top-level parameter SSLWebServicePort in the ClientAdapter configuration to true (*true is the default*).
- In the ClientAdapter, for DIVA API socket connections. To enable (*you must be using DIVA API version 7.6 or greater*), set the parameter SSLSocket in the ApiPorts section of the ClientAdapter configuration to true.

- In the ManagerAdapter, for web service connections. To enable, set the top-level parameter SSLWebServicePort in the ManagerAdapter configuration to true (*true is the default*).
- In the ManagerAdapter, for the socket connection to the DIVA Manager. To enable, set the top-level parameter ManagerSSLSocket to true (*DIVA 7.6 or greater is required*).
- In the DbSync service, for web service connections. To enable, set the top-level parameter SSLWebServicePort in the DbSync configuration to true (*true is the default*).
- In the connection to the Oracle database. To enable, in the database section of DIVA Connect configuration files, set the parameter SecureMode to 1. You may need to set the cipher suite "SSL_DH_anon_WITH_3DES_EDE_CBC_SHA" in the Oracle listener configuration. In this release, DIVA Connect does not support database authentication using SSL.

DIVA Connect contains certificate data in two places: a *private keystore*, used for web services hosted on the local system, and a *public keystore*, used to verify web services that are invoked remotely. You can use the Java Keytool Utility to change the keystore password and add and delete certificates.

Refer to the following for more information regarding creating keystores:

http://docs.oracle.com/javase/8/docs/technotes/guides/security/jsse/JSSERefGuide.html#CreateKeystore

Private Keystore

For DIVA Connect web services, private key certificate data is stored in:

$DIVA Connect_HOME/Program/divaconnect/lib/diva129.jks

Exactly one certificate must appear in this keystore. This certificate is used for web services hosted by services running from this $DIVA Connect_HOME directory. It is recommended to replace the shipped certificate with a new certificate, and use a different certificate for each DIVA Connect site in your network.

You must change the password of this keystore. Store the password information in a new file named $DIVA Connect_HOME/Program/divaconnect/lib/diva129.properties, and make this file readable by DIVA Connect services (*in Linux this user is divaconnectsvc*), but not readable by casual users of the system (*for example, the diva user in Linux*). Use the following format for the file:

keystorePassword=*newpassword*

To configure DIVA API socket connections certificates in the DIVA Connect product, see the DIVA Core 7.7 Security Guide.

Public Keystore

Sometimes referred to as the *truststore* for web services, this data is located in:

$DIVA Connect_HOME/Java/lib/security/cacerts2

This certificate data is used in outbound web service calls (*including DIVA ConnectUI*). Multiple public keys can be loaded into this keystore.

If you added a new self-signed certificate into the DIVA Connect private keystore, export the certificate using the keytool utility. All of the applications (*DIVA Connect services, DIVA ConnectUI, and so on*) that invoke WebServices on this site should then add the exported certificate to their own public keystore.

Refer to the DIVA Core 7.7 Security Guide for information about the public keystore for DIVA API socket connections.

A

Secure Deployment Checklist

1. Set strong passwords for the Administrator and any other operating system accounts that have any DIVA Connect administrator or service roles assigned to them. This includes:
   - diva, divaconnectsvc, and Oracle User IDs if being used
   - Any disk administrative accounts
2. Do not use a local administrator operating system account, instead assign roles as needed to other user accounts.
3. Use site-specific certificates for each DIVA Connect installation, and define a strong password for the Oracle database and private keystore. Set a strong password for the Oracle database operating system login.
4. Install firewall software on every DIVA Connect system and apply the default DIVA Connect port rules. Restrict access to the DIVA Connect API socket (*tcp 7101*) to IPs that require access using firewall rules. Perform this step with DIVA Connect's Access Rules.
5. Install operating system and DIVA Connect updates on a periodic basis since they include security patches.
6. Install antivirus and exclude the DIVA View processes and storage for performance reasons.
7. Best practices dictate segregation of 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. This security practice helps prevent loss-of-data accidents resulting from accidental overwriting important data.
8. Configure an appropriate set of backups for the DIVA Connect configuration and database. Backups are part of security and provide a way of restoring data lost either accidentally, or through some breach. Your backup should include some policy while being transported to an off-site location. Backups need to be protected to the same degree as DIVA Connect disks.