Cerify
Automated Video Content Verification System

Quick Start User Manual

Tektronix

**Cerify
Automated Video Content Verification System**

Quick Start User Manual

Tektronix

Cerify Technical Support

To obtain technical support for your Cerify system, send an e-mail to the following address: cerify-support@tek.com.

Contacting Tektronix

Tektronix, Inc.
14150 SW Karl Braun Drive
P.O. Box 500
Beaverton, OR 97077
USA

For product information, sales, service, and technical support:
- In North America, call 1-800-833-9200.
- Worldwide, visit www.tektronix.com to find contacts in your area.

Warranty

Tektronix warrants that the media on which this software product is furnished and the encoding of the programs on the media will be free from defects in materials and workmanship for a period of three (3) months from the date of shipment. If any such medium or encoding proves defective during the warranty period, Tektronix will provide a replacement in exchange for the defective medium. Except as to the media on which this software product is furnished, this software product is provided "as is" without warranty of any kind, either express or implied. Tektronix does not warrant that the functions contained in this software product will meet Customer's requirements or that the operation of the programs will be uninterrupted or error-free.

In order to obtain service under this warranty, Customer must notify Tektronix of the defect before the expiration of the warranty period. If Tektronix is unable to provide a replacement that is free from defects in materials and workmanship within a reasonable time thereafter, Customer may terminate the license for this software product and return this software product and any associated materials for credit or refund.

THIS WARRANTY IS GIVEN BY TEKTRONIX WITH RESPECT TO THE PRODUCT IN LIEU OF ANY OTHER WARRANTIES, EXPRESS OR IMPLIED. TEKTRONIX AND ITS VENDORS DISCLAIM ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. TEKTRONIX' RESPONSIBILITY TO REPLACE DEFECTIVE MEDIA OR REFUND CUSTOMER'S PAYMENT IS THE SOLE AND EXCLUSIVE REMEDY PROVIDED TO THE CUSTOMER FOR BREACH OF THIS WARRANTY. TEKTRONIX AND ITS VENDORS WILL NOT BE LIABLE FOR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES IRRESPECTIVE OF WHETHER TEKTRONIX OR THE VENDOR HAS ADVANCE NOTICE OF THE POSSIBILITY OF SUCH DAMAGES.

[W9b – 15AUG04]

Table of Contents

Environmental considerations

Product end-of-life handling

Observe the following guidelines when recycling an instrument or component:

This section provides information about the environmental impact of the product.

Equipment recycling

Production of this equipment required the extraction and use of natural resources. The equipment may contain substances that could be harmful to the environment or human health if improperly handled at the product's end of life. In order to avoid release of such substances into the environment and to reduce the use of natural resources, we encourage you to recycle this product in an appropriate system that will ensure that most of the materials are reused or recycled appropriately.

This symbol indicates that this product complies with the applicable European Union requirements according to Directives 2002/96/EC and 2006/66/EC on waste electrical and electronic equipment (WEEE) and batteries. For information about recycling options, check the Support/Service section of the Tektronix Web site (www.tektronix.com).

Perchlorate materials. This product contains one or more type CR lithium batteries. According to the state of California, CR lithium batteries are classified as perchlorate materials and require special handling. See www.dtsc.ca.gov/hazardouswaste/perchlorate for additional information.

Preface

The Cerify application is an automated system for testing compressed digital media. This manual provides installation instructions and a high-level operational overview of this product.

Product description

The Cerify software checks file-based digital audio/video content in a consistent and configurable manner. Files can be checked for correct digital encoding and against baseband quality parameters. Cerify provides both broadcast and production operations with a fast, cost effective QC solution.

The Cerify system can be integrated with your existing infrastructure using the CeriTalk API to interface with asset management systems and provide a completely automated workflow. A Web-based user interface allows test results to be viewed from any network connected workstation.

System components

Cerify accesses digital media from local storage, such as a local hard drive or DVD, as well as network storage, such as a Windows file server or FTP server.

A Cerify system can be set up in three basic ways:

■ The first consists of a single self-contained unit which runs all the management and testing processes of the system.

■ The second consists of a networked cluster of two or more units, which enables simultaneous processing of a greater number of files. The networked cluster contains a single Supervisor and one or more Media Test Units.

■ The third consists of a cluster of three or more units with high availability (HA) support. Cerify Enterprise Cluster with high availability (also referred to as an HA cluster) is a Cerify cluster enabled with support in the case of a Supervisor system failure.

License dongle

The license dongle must be plugged into the USB port on your computer to run the application. In a clustered system, Media Test Units acquire their licenses from the Supervisor.

In the case of an HA cluster, two identical license dongles are supplied. The two dongles need to be inserted in the USB ports of the primary and secondary supervisors. Media Test Units will acquire licenses from the active primary Supervisor.

Figure i: License dongle

It is possible to navigate the user interface and see previous results when no dongle is installed, but it is not possible to carry out new checks of digital media files. The license dongle controls:

- The types of codecs and file formats that can be checked

- The number of channels that can be used

- For demo dongles, when the license will expire

- Server configuration (Supervisor, Secondary Supervisor or Media Test Unit, High Availability cluster or not, etc.)

NOTE. If you unplug a dongle and plug in another dongle, or if the connected dongle is upgraded with a new v2c file, a restart of Cerify is necessary for the license dongle to work correctly.

When you install a new version of the Cerify software for a high availability (HA) cluster, both of the dongles connected to the primary and secondary Supervisors must be upgraded.

Networking

In a clustered configuration, network interface on all of the units, including the Supervisor, secondary Supervisor (HA cluster only) and Media Test Units, should be connected to the local area network. This connection is used to access media files, to service Web clients, and to carry cluster control traffic.
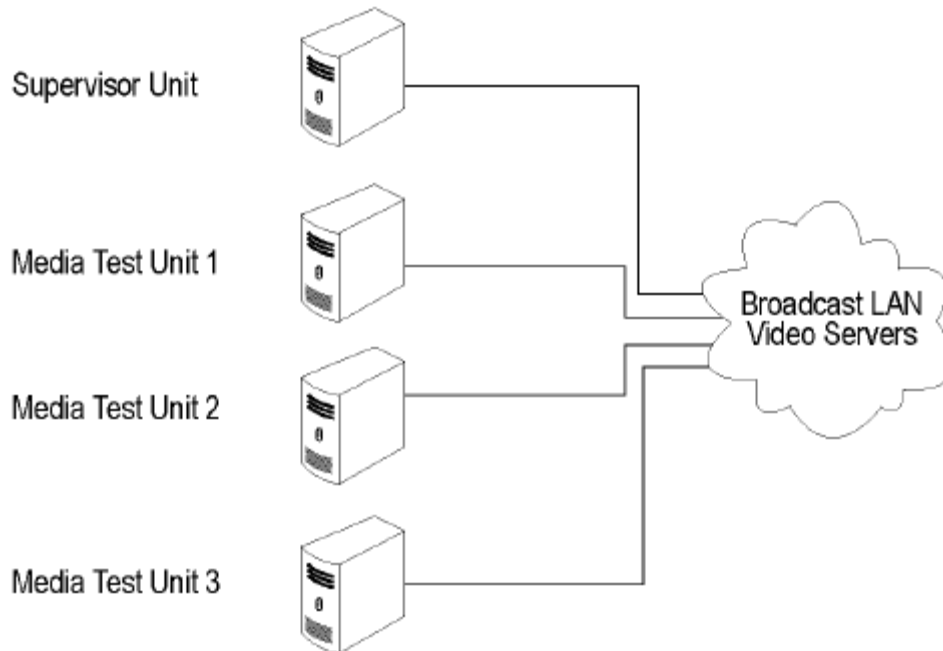

Figure ii: Clustering topology

Software components

Software components include:

- A Web-based user interface, which allows users to create and control Jobs, and to view or report the results of these Jobs. This interface is accessed over the network by using a Web browser. All you need to know is the IP address of your unit.

- Media test service, which performs media file verification according to the rules chosen by the user.

- A database, which provides robust storage of the system entities, including users, Jobs, and Job results.

- An XML-based control and reporting API known as CeriTalk. CeriTalk allows interaction with Cerify from within other applications, making it possible to integrate Cerify with other content management, broadcast automation, and workflow systems.

- A Web application server that provides access to the Web interface and runs the core services for the application.

- A license server, which controls the types of files that can be verified.

- The system tray icon and menu, which provides access to the Cerify Web-based user interface and allows the application to be started and stopped. The system tray icon is not available when Cerify is installed as a Windows service.

Cerify as a standalone system

A standalone system is a single machine that combines the functions of a Supervisor unit and a Media Test Unit. The process that carries out the media file testing is known as the Media Test Client (MTC).

Cerify enterprise cluster

The Supervisor unit controls the cluster system. It hosts the database and the Web server, allowing multiple users to set up and view Jobs. It is responsible for locating the media files from the network, but delegates actual transfer and processing of these files to one or more Media Test Units. The Supervisor unit organizes and stores the resulting outputs.

Each Media Test Unit is responsible for processing the digital media files in a networked cluster. It applies the user-specified tests, and reports back the results. The Supervisor can also be configured to process the files.
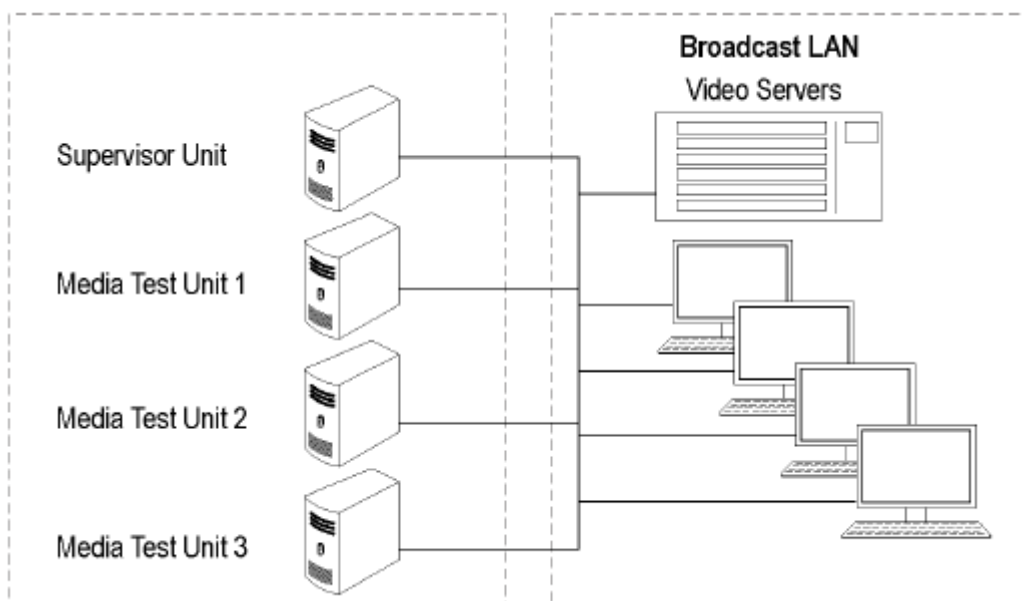

Figure iii: Local area networking

Cerify high availability enterprise cluster

The Cerify high availability enterprise cluster (also referred to as an HA cluster) is a Cerify cluster enabled with support in the case of a Supervisor system failure. In an HA cluster, one of the member units of the cluster is configured as a backup to the Primary Supervisor and is called the Secondary Supervisor.

If Cerify on the Primary Supervisor goes down for any reason (for example, due to a machine crash), the Secondary Supervisor automatically takes over and manages the cluster. All other units (MTUs) now form a cluster with the Secondary Supervisor. Once the Primary Supervisor recovers, it will assume the role of the Secondary Supervisor and will be ready to take over when the current Supervisor goes down.

The Secondary Supervisor is a part of the HA cluster and can also process files like the Primary Supervisor and the MTUs in the cluster while performing the job of a Secondary Supervisor.

In an HA cluster, it is mandatory for the Primary Supervisor and Secondary Supervisor to have two network interface cards on the system. One will be used for the cluster function and the other for communication (Ceritalk/Web). Also, it is mandatory to use static IP addresses for all the units forming the HA cluster.

In an HA cluster, identical dongles must be connected to the Primary Supervisor and Secondary Supervisor. When starting an HA cluster, the cluster units should be started in the following order:

1. The Primary Supervisor should be started first with one of the two HA dongles installed. At the time the Primary Supervisor is started, the system with the Secondary Supervisor installed should be up and have the matching HA dongle installed. Otherwise, the Primary Supervisor will not start.

2. The Secondary Supervisor should be started next.

3. The Media Test Units should be started one by one after both the Primary Supervisor and Secondary Supervisor are started.

System requirements

The system must meet the following hardware and software prerequisites:

Hardware prerequisites

Cerify runs on a variety of PC hardware. Consequently, the choice of hardware is determined by performance and throughput requirements for your installation. This section recommends hardware configuration for some scenarios in which Cerify is typically used.

Cerify can be installed as either of the following two configurations on a given computer:

- Single channel. A single channel installation is one that is licensed to test a single media file at a time. Such installations are normally performed on a PC or a laptop computer and are suitable for situations where a low throughput is sufficient and performance is not critical.

- Multichannel. A typical multichannel installation of Cerify tests 4-8 media files at a time on a single unit. Due to the high throughput and performance requirements that are expected from such installations, it is recommended that server class hardware and operating systems be used in such cases.

In addition to the throughput required, the hardware requirements for such installations also depend heavily on the mode of operation that will be used. For more information on the modes of operation of Cerify, refer to the *Modes of Operation* section in the Cerify User Manual.

The general guidelines that should be followed when selecting hardware are:

- Processor: 3 GHz

  Cerify is capable of using as many processor cores as available for improved processing performance. While the minimum required configuration is 2 cores per channel, for optimum performance, it is recommended to allocate between 4 and 6 processor cores per Cerify channel. It is also recommended that for best performance, you choose as much on-chip memory cache as possible.

NOTE. Cerify is optimized for Intel processor architectures, and therefore it is recommended that you use an Intel based server platform.

- Memory:

  It is recommended to use a minimum of 4 GB of RAM per channel and an additional 4 GB for the operating system and the Cerify database. For optimum performance for 4 channels, the recommended memory therefore is: 4 x 4 GB (per channel) + 4 GB = 20 GB. When the expected load in Cerify is likely to be largely composed of huge media files, more memory per channel may be necessary.

■ Hard disk drive: 100 GB x 3

For an enterprise installation, we recommend using a RAID on which to place the MS Windows and Cerify installation (including database) to achieve fault tolerance in case of disk failure. This logical drive should be at least 100 GB in size. For systems that are expected to support high levels of throughput, it is recommended that you have 500 GB of space on this logical drive.

The amount of additional storage you need depends on the mode of operation that applies to your installation, the average size of the files you will be processing, and the number of channels you will be running.

- Streaming mode

  Due to the minimal hard disk utilization when operating in the streaming mode, it is sufficient to provide a single dedicated hard disk of 100 GB in size as temporary storage for Cerify.

- Copying mode

  The minimum hard disk space provided must be greater than the average file size being processed multiplied by the number of channels. It is recommended that the temporary storage be RAID-ed for better performance.

Choose the optimal number of hard disks for your installation and the best RAID levels to use. For help in choosing the optimal number of hard disks for your installation and the best RAID levles to use, see the "Configuring Your Cerify Installation for Best Performance" section in the Cerify user manual.

■ Network interface: 1 Gbit/s

You might use multiple network interfaces to improve available network bandwidth

■ Integrated RAID controller

■ A DVD drive (used for installing the software)

■ A USB port for connecting the license dongle

■ A license dongle (provided with the product)

■ Redundant power supply

For more detailed specification of a validated enterprise PC platform, see "Commercial off-the-Shelf Recommendations" section under Appendix E: Configuring Your Cerify Installation of the Cerify user manual.

Supported platforms

■ Windows 7 - 64 bit

■ Windows Server 2008 64-bit

■ Windows Server 2008 R2 64-bit

NOTE. Cerify is expected to operate correctly on other variants of Windows as well, but it has been qualified only on the ones specified above.

Apple ProRes, Generic QuickTime and JPEG 2000 Video decoding functions are not available on Microsoft Windows XP 64 bit and Windows Server 2003 because of known compatibility issues with QuickTime Player.

Software prerequisites

The computer on which the application is installed will need the following:

- To run one of the supported platforms.

- To access the system through its Web user interface from another computer on the network, the client computer must have a Web browser installed.

NOTE. To access the application, the preferred Web browser is Microsoft Internet Explorer (version 7.0 and above). The application has also been tested with Mozilla Firefox. There may be minor visual differences in the appearance of the user interface in different Web browsers.

Clustering requirements

A cluster is a network of two or more units, which enables simultaneous processing of a greater number of files. The networked cluster contains a single Supervisor and one or more Media Test Units.

The Supervisor unit controls the cluster system. It hosts the database and the Web server, allowing multiple users to set up and view Jobs. It is responsible for locating the media files from the network, but delegates actual transfer and processing of these files to one or more Media Test Units. The Supervisor unit organizes and stores the resulting outputs. The Supervisor can also be configured to process the media files.

The Media Test Unit is responsible for processing of the digital media files in a cluster. It applies the user-specified tests and reports results the back to the Supervisor unit.

To set up a cluster, install Media Test Units and Supervisor on the respective nodes.

Cluster system requirements

- Two or more PCs with 64-bit Windows Server 2008 SE OS installed.

- Administrator privileges on all the machines on which the Cerify software will be installed.

- All of the systems with Cerify installed need to meet the minimum hardware specifications.

- All of the clustering PCs, Media Test Units, and Secondary Supervisor unit should reside on the same network as the Supervisor unit. It is recommended that each cluster unit be configured with Static IP addresses.

- All of the PCs in the cluster should be able to route to each other. The Supervisor unit and the Secondary Supervisor unit (in the case of an HA cluster) each need to be given a network name that is recognized and resolved by all of the units in the cluster.

- You should know the fully qualified name of the Supervisor unit and the Secondary Supervisor unit and provide these when the installer of the other units in the cluster asks for the names of the Supervisor and Secondary Supervisor units.

- In the case of a normal cluster (non-HA cluster), if the Supervisor or Media Test Units have more than one network interfaces, it is better to bridge all the network interfaces together. (See page 6, *Configuring a network bridge.*)

- Synchronization between all the units in cluster must be maintained. For example, use an NTP server to synchronize the units in a cluster.

- All the units in the cluster should be configured to be in the same time zone.

Clustering scenarios which may not work

Clusters may not work in the following scenarios:

■ If the Supervisor, the Secondary Supervisor (in the case of an HA cluster), and the Media Test Unit are in different subnets wherein the switch blocks the multicast or UDP traffic.

■ If any of Supervisor, Secondary Supervisor, or Media Test Unit systems has Windows firewall running, the Firewall may need some additional configurations for the cluster to work. Contact your Tektronix representative for more information on how to set up this configuration.

■ If a Media Test Unit or Secondary Supervisor cannot resolve Supervisor host name.

■ In the case of an HA cluster, if the Supervisor can not resolve the host name of the Secondary Supervisor and vice versa.

■ If the Supervisor does not have a host name or if the Supervisor has a host name with Japanese or Chinese characters.

■ If a network has another system with the same host name as the Supervisor (or Secondary Supervisor) system.

■ If the host name of the Supervisor (or Secondary Supervisor) changes after cluster installation.

■ If the http port on the Supervisor is configured to a different port number after cluster installation. In this case, the property cerify.supervisor.httpport in the cerifysystem.properties on the Media Test Units must be changed to the new port number.

■ If the http port on the Supervisor is configured differently than that of the Secondary Supervisor.

■ If the IP addresses of any units in the cluster change after the installation. In this case, the property cerify.jboss.bindaddress must to be changed to the current IP address.

■ In the case of a normal (non-HA) cluster, if the Supervisor has multiple network interfaces connected to the same network and if DNS/WINS are not configured properly, troubleshoot this problem by doing either of the following:

  – By adding an entry containing the Supervisor host name and the IP address used by Cerify on Supervisor in "hosts" file, which can be found in `C:\WINDOWS\system32\drivers\etc` in all the Media Test Units.

  – By bridging all the network interfaces together.

■ Clusters might not work correctly if there is momentary network outage in which case the clusters have to be restarted.

Related documentation

The following documents are available:

■ Cerify Online Help

■ Cerify User Manual (Tektronix part number, 077-0352-xx)

■ Cerify Release Notes (Tektronix part number, 077-0752-xx)

■ Cerify Third Party Software License Notice Document (Tektronix part number, 001-1513-xx)

■ Cerify Upgrades Read This First (Tektronix part number, 061-4355-xx)

Installation

Before installation

Network connection

Before installing the Cerify application, your PC must be correctly connected to your local network.

This allows the following:

- The Cerify application to test the files that are available on other machines on the network.

- Other machines to interact with Cerify automatically (for example, using CeriTalk automation clients, copying of report files to network locations, or using email).

- Multiple users to connect to the Cerify Web user interface from remote computers.

For the last two cases, you need to know the IP address or the network name of the machine that Cerify is installed on. Network settings on the PC are configured in the usual manner using Windows. If your machine is not properly configured or you do not know the name or IP address information, contact your system administrator.

Installation considerations

Before installing Cerify, you should be aware of the following information:

- It is recommended that the Cerify application be installed on a machine where it can be used as the sole running application. Cerify makes intensive use of both CPU and memory and will considerably degrade the performance of other running applications. Similarly, running other applications or services simultaneously will degrade the performance of Cerify and increase the time taken to process a media file.

- Cerify relies on third-party software applications that are packaged and installed with it: JBoss and MySQL. If these applications are already used on the PC, you should remove them before attempting to install the Cerify.

- The Cerify license server relies on Sentinel HASP (formerly Aladdin HASP SRM) drivers, which are installed and configured along with it. It is recommended that other applications that rely on HASP licenses not be used with Cerify on the same machine.

- Cerify uses a number of network services that are local to the host PC. These services can sometimes be blocked by personal firewall software, in which case an error message will be displayed when Cerify starts. For example, on Cerify start up, a check is made to verify that communication with HASP can be established. If the Cerify application is unable to communicate with HASP, an error message, **Unable to connect to HASP License Manager (port 1947). Please check if the HASP License Manager service is running and is not blocked by a firewall** is displayed and Cerify is stopped.

  In such situations, configure the firewall to allow the service on the appropriate port, or alternatively disable the firewall entirely.

- An installation log is written to the "%userprofile%\Cerify\CerifyInstallationLogs_<Timestamp>" folder. This log gives details of selections you made during the install and any errors encountered in case of failure to install.

- If you would like multiple users to be able to run the Cerify application on the PC, make sure you select a location that has read and write permissions for those users as the temporary video folder. A directory located within a user's private directory is not suitable in this case.

- While choosing the location for storing temporary video files during installation, make sure that there is sufficient free space in this folder to store large video files

- Cerify uses the computer name (as stored in the environment variable named "COMPUTERNAME") to uniquely identify some of its network services. This will not work if non-ASCII characters are used in the computer name.

- Cerify will fail to run if any other Web services using port 80 are running on the system where the Cerify is installed (for example, the IIS Admin service, Skype or Apache). You can run Cerify once you shut down the other port 80 services running on the system. Alternatively, you can configure the Cerify Web port to use a port other than 80.

- It is not possible to install a lower version of Cerify when you have a higher version of Cerify already installed. For example, if you install Cerify version 6.1 and then you want to go back to Cerify version 6.0, you will need to first uninstall Cerify 6.1 and then install Cerify 6.0.

Software installation

The installation of the Cerify application takes several minutes; typically between 5 and 15 minutes depending on the speed of your PC.

⚠ *CAUTION. To prevent installation problems, be sure to read about the known installation limitations. (See page 1, Installation considerations.)*

To install Cerify, you need to perform the following steps:

1. Run the Cerify Installer.

2. Insert the Cerify dongle(s).

3. *Optional*: Install Apple QuickTime Player.

Running the Cerify installer

To run the Cerify installer, do the following:

- Ensure that you are logged in as a user with administrator privileges.

NOTE. If you try to install the Cerify application without administrator privileges, the following message appears: "The Cerify application can be installed or uninstalled only by a system administrator. Please log in as administrator and try again".

- Insert the Cerify DVD provided by Tektronix. The Cerify Application Browser opens. Click the **Install Cerify** link to launch the Cerify installer. Follow the on-screen instructions to perform the installation.

NOTE. If you try to install the Cerify application on an unsupported platform (See page ix, Supported platforms.), then the following message appears: "This is not a supported Windows operating system. Cerify will probably operate correctly but has not been validated on this OS. Do you wish to continue installation?"

The Cerify installation will not continue on a Windows XP platform. The installer displays a message saying Windows XP is not supported and the installation is aborted.

If the browser does not open automatically, or if the **Install Cerify** link does not work, navigate to the Exec folder located on the Cerify Software Installation DVD and double-click **CerifySetup<version>.exe**. Follow the on-screen instructions to perform the installation.

A number of third party software applications are installed during the installation process. Most of these are not visible, but you will be notified as the WinPcap and HASP drivers are installed.

NOTE. WinPcap is not used in the normal operation of the Cerify application. It is used when you collect support diagnostics to troubleshoot networking issues with Cerify.

Installation options

Cerify can be installed in the following ways:

- Standalone

- Supervisor (for an Enterprise cluster): The Supervisor unit controls the cluster system. It hosts the database and the Web server, allowing multiple users to set up and view Jobs. Use this option to install the Supervisor for a normal cluster (without high availability support).

- Media Test Unit (for an Enterprise cluster): Each Media Test Unit is responsible for processing the digital media files in a networked cluster. Use this option to install Media Test Units for a normal cluster (without high availability support).

- Supervisor (for an HA cluster): Use this option to install the Primary Supervisor for an HA (high availability) cluster.

- Secondary Supervisor (for an HA cluster): Use this option to install a Secondary Supervisor for an HA (high availability) cluster, which will act as the Primary Supervisor if the Primary Supervisor system goes down.

- Media Test Unit (for an HA cluster): Use this option to install Media Test Units for an HA (high availability) cluster.

NOTE. During the installation of Cerify, if there are multiple network interfaces in the system, the installer provides the list of network interfaces and asks the user to select a network interface to be used by Cerify.

While installing the Supervisor and the Secondary Supervisor (in the case of an HA cluster), the installer also provides the option to select the network interface for communication (i.e. the interface used for communicating with Cerify via either Ceritalk or the Web user interface).

The installer also provides an option to install Cerify as a service. This option is selected by default. If you want to install Cerify in application mode, this option needs to be deselected.

Installing Cerify as a Supervisor.   To install Cerify as a Supervisor, follow the steps described in *Running the Cerify installer*. (See page 2.) During the installation, a dialog box appears with the list of installation options.

To continue with the Supervisor installation for a normal Enterprise cluster, select **Supervisor** under the option "Enterprise Cluster" in the installation options dialog box.

To install the Supervisor for an HA cluster, select **Supervisor** under the option "High Availability Enterprise Cluster" in the installation options dialog box.

During the installation, a dialog box appears where you must:

- Enable or disable file-processing option on the Supervisor.

- Enter the number of channels if you have selected the file processing option on the Supervisor.

- Choose the network interface to be used by Cerify.

- Choose the network interface to be used for all Cerify communication. This option is available only while installing the Supervisor for an HA cluster.

- Enter the host name of the Secondary Supervisor. This option is available only while installing the Supervisor for an HA cluster.

- Enter the host names for all the Media Test Units if you want to install the cluster based on unicast communication since most of the switches drop multicast packets.

At the end of the installation, the installer prompts you with an option to load the demo content. If you choose this option, Cerify will be loaded with a demo database, which will contain some sample jobs with results.

Installing Cerify as a Secondary Supervisor.   Follow the steps described in *Running the Cerify installer* (See page 2.) to install Cerify as a Secondary Supervisor for an HA cluster. During the installation, a dialog box appears with the list of installation options.

To continue with the Secondary Supervisor installation, select **Secondary Supervisor** under the option "High Availability Enterprise Cluster" in the installation options dialog box.

During the installation, a dialog box appears where you must:

- Enable or disable the file-processing option on the Secondary Supervisor.

- Enter the number of channels if you have selected the file processing option on the Secondary Supervisor.

- Choose the network interface to be used by Cerify.

- Choose the network interface to be used for all Cerify communication.

- Enter the host name of the Supervisor.

- Enter the host names for all of the Media Test Units if you want to install the HA cluster based on unicast communication since most of the switches drop multicast packets.

Installing Cerify as a Media Test Unit. Follow the steps described in *Running the Cerify installer* section to install Cerify as an Media Test Unit.(See page 2.) During the installation, a dialog box appears with the list of installation options.

To continue with the Media Test Unit installation for a normal Enterprise cluster, select **Media Test Unit** under the "Enterprise Cluster" option in the installation options dialog box.

To continue with the Media Test Unit installation for an HA cluster, select **Media Test Unit** under the "High Availability Enterprise Cluster" option in the installation options dialog box.

During the installation, a dialog box appears where you must:

- Enter Host name of the Supervisor.

- Enter the host name of the Secondary Supervisor. This option is available only while installing Media Test Unit for an HA cluster.

- Choose the network interface to be used by Cerify.

- Enter the number of channels.

Configuring a non-HA cluster. To configure a non-HA cluster, you must:

- Install Cerify as a Supervisor on the system which must be configured as supervisor of the cluster.

- Install Cerify as a Media Test Unit on one or more systems.

When installing Cerify as a Media Test Unit, the installer prompts you to enter the Supervisor host name. The installer checks whether the Media Test Unit can reach the Supervisor system using the host name entered. If the Supervisor system cannot be reached, a message appears whether you still want to continue the installation.

You can also configure multiple clusters on the same network. To configure multiple clusters on the same network, you need to install multiple Supervisors. During a Media Test Unit installation, in the Cerify System Settings dialog box, you must enter the respective Supervisor host name.

*NOTE. To configure a cluster, the versions of Cerify on the Supervisor and the Media Test Unit should be the same. Once the installation is complete, Cerify will be started on both the Supervisor and the Media Test Unit. Access Supervisor using Cerify Web UI and navigate to the Admin page, click the **Media Test Units** link to the page containing the list of Media Test Units.*

Configuring an HA Cluster. To configure an HA (high availability) cluster, you must:

- Install Cerify as a Supervisor by choosing **Supervisor** under the "High Availability Enterprise Cluster" option on the system that is to be configured as the Primary Supervisor of the cluster.

- Install Cerify as a Secondary Supervisor by choosing **Secondary Supervisor** under the "High Availability Enterprise Cluster" option on the system that is to be configured as the Secondary Supervisor of the cluster.

- Install Cerify as a Media Test Unit by choosing **Media Test Unit** under the "High Availability Enterprise Cluster" option on one or more systems.

When installing Cerify as a Media Test Unit for an HA cluster, the installer prompts you to enter the host names of the Supervisor and Secondary Supervisor systems. The installer checks whether the Media Test Unit can reach the Supervisor and Secondary Supervisor systems using the host names that you entered. If either the Supervisor or Secondary Supervisor system cannot be reached, a message appears asking whether you still want to continue the installation.

NOTE. To configure an HA cluster, the version of Cerify that is installed on the Supervisor, Secondary Supervisor, and the Media Test Units should be the same. Once the installation is complete, Cerify will be started on the Supervisor, Secondary Supervisor, and the Media Test Units. Access the Supervisor using the Cerify Web UI and navigate to the Admin page. Click the Media Test Units link to the page containing the list of Media Test Units.

Configuring a network bridge

If the system has multiple network adapters, it is recommend that you bridge all the network adapters.

1. From the Start menu, select **Control Panel** > **Network Connections**.

2. Select two network adapters at the same time, right-click and select **Bridge Connections**. Windows will build up a network bridge automatically. When the bridge is built successfully, the two adapters' IP address disappears.

3. Select the **Network Bridge** and configure a new IP address in the **Properties** menu for LAN connections.

*NOTE. To configure a cluster, the versions of the supervisor and the Media Test Unit should be the same. Once the installation is complete, Cerify will be started on both Supervisor and Media Test Unit. You can access Supervisor using Cerify Web UI and navigate to the Admin page on Web UI, Click the **Media Test Unit Details** link to the page containing the list of Media Test Units.*

Installation folders

During the installation process, select the following locations:

- **Installation Location**: The folder where the application is installed.

- **Temporary Storage Location**: Before processing media files from an external server, Cerify may need to copy the remote files to the PC on which the Cerify application is installed. This folder is used as the location to store such temporary copies. Cerify copies the file only when operating in copy mode and accesses the file using the ftp://, smb://, or gvg:// protocols. See *Modes of Operation* in *Appendix E* of the *Cerify User Manual* for help determining the mode that applies to your installation.

NOTE. There should be sufficient free space in the temp folder to store large video files. The location for this temp folder can be on any drive on the computer.

If you would like multiple users to be able to run the Cerify application on the PC, make sure to select a location that has read and write permissions for those users. A temporary directory located within a users private directory is not suitable in this case.

Inserting the Cerify dongle

Insert the Cerify license dongle supplied with the system in any of the available USB ports of your computer. In the case of normal Enterprise cluster, the dongle should be inserted in the USB port of the Supervisor system. In the case of an HA cluster, you will be supplied with two identical dongles. The two dongles should be inserted in the USB port of both the Supervisor and Secondary Supervisor systems.

NOTE. Do not insert the dongle before the Cerify installation. Insert the dongle only when the installer prompts you.

NOTE. If Cerify reports license failures after the dongle has been installed, it is possible that firewall software is interfering with the license service. Please ensure that port 1947 is open in any firewall software that is in use. See Licensing limitations for a list of other possible causes of license failures. (See page 8.)

The number of files that can be simultaneously processed by Cerify will be the number of allowed channels specified in the dongle. If a time-expiry dongle is connected, the default number of files processed is 1.

Sometimes, you will need to change the number of files that can be simultaneously processed by Cerify. You can change the number of parallel processing channel setting by changing the value of the property "cerify.processorsperbox" in the "cerifysystem.properties" file located at `<Installation Directory>/Cerify/JBoss/server/all/conf`.

The following lists the different situations for standalone installation:

- When Cerify is started with no dongle connected, then (irrespective of whether a value has been specified in the "cerify.processorsperbox" property or not) the number of allowed channels is zero.

- When Cerify is started with a perpetually licensed dongle and if the "cerify.processorsperbox" property is not set then the number of allowed channels is controlled by the dongle.

- When Cerify is started with any valid dongle and a valid number of channels is specified for the "cerify.processorsperbox" property, then this value would be used if it is less than or equal to the number of channels controlled by the dongle. If the value is greater than the number of channels controlled by the dongle then the number of channels controlled by the dongle takes precedence.

■ When Cerify is started with any valid dongle and the number of channels specified for the "cerify.processorsperbox" property is -1, then the number of allowed channels is controlled by the dongle.

■ When Cerify is started with a time-expired dongle and if the "cerify.processorsperbox" property is not set, then the number of allowed channels is set to 1.

Installing Apple QuickTime Player

To process Apple ProRes files using the Generic QuickTime Video template or to process files using the JPEG 2000 Video templates, you have to install QuickTime Player. Download QuickTime player from the link: www.apple.com/quicktime/download/.

NOTE. If you already have QuickTime Player installed, make sure that it is version 7.5.5 or later.

Licensing limitations

The following limitations may affect the ability to license Cerify:

■ The Cerify 6.0 or later software requires the use of a HASP NetTime dongle. It is not possible to use a HASP Net dongle (as used with Cerify 5.x and earlier) without updating the dongle firmware. Green HASP Max dongles (as used with CerifyLite) are no longer supported.

■ When multiple HASP license servers are available on the network, there is a chance that the Cerify unit will try to retrieve its license from a wrong server and fail to obtain the required features, resulting in licensing errors.

■ It is possible to insert the HASP license dongle into a different machine from that on which Cerify is installed. This might be desirable if the Cerify hardware does not have a USB port - e.g. blade hardware. Contact your Tektronix representative for more information on how to do this.

■ It is possible for the license server to retain handles to license features that were being used by a Cerify machine that has suddenly lost power or otherwise failed. As a result of this the Cerify application will not be able to obtain a license until the license server is restarted. This will only be a problem when the license dongle is not on the Cerify machine, so in this configuration we recommend that the license server machine is restarted when the Cerify application is restarted.

■ If Cerify reports license failures after the dongle has been installed, it is possible that firewall software is interfering with the license service. Please ensure that port 1947 is open in any firewall software that is in use.

Software uninstallation

Before uninstallation, ensure that you have administrator privileges. If you try to uninstall Cerify without administrator privileges, the uninstallation process will be aborted.

Cerify can be uninstalled in two ways:

- Through **Start** > **Control Panel** > **Add or Remove Programs**.

- By rerunning the **CerifySetup<version>.exe** that you used to install the current version and following the on-screen instructions.

NOTE. If the Cerify installer version is higher than the currently installed version, the installation will be upgraded to the newer version.

If the Cerify installer version is lower than the current installed version, the installer will abort without taking any action.

*NOTE. The Cerify installation process places the WinPCap and HASP utilities in the **Add or Remove Programs** list. The uninstallation process does not remove WinPCap in case it is being used by other programs or you want to continue to use it for other purposes. The HASP drivers are uninstalled. If you want to uninstall WinPCap, this can be done in the usual way from the **Add or Remove Programs** list.*

*NOTE. If you select the **Backup database** option during uninstallation, the current database will be backed up to `C:\Doc-uments and Settings\<username>\Cerify\CerifyBackup_<version>_<timestamp>`. You are given the option to change the directory where you want to back up the database. All relevant configuration files will be backed up to `C:\Documents and Settings\<username>\Cerify\CerifyConfig_<version>_<timestamp>`. The "Backup database" option will not be available if you are uninstalling the Media Test Unit, as the Media Test Unit does not have its own database.*

*NOTE. If Cerify 6.0 is uninstalled using **Add or Remove Programs** option or using Cerify 6.0 installer, there will be no "backup" option. The Cerify database and configuration files will always be backed up at the location `C:\Documents and Settings\<username>\Cerify\CerifyBackup`. When Cerify 7.x is installed, the installer will change the directory name "CerifyBackup" to "CerifyBackup_6.0".*

Uninstalling a cluster

To uninstall a cluster, do the following:

- Uninstall Cerify on the Supervisor.

- Uninstall Cerify on the Secondary Supervisor (in the case of an HA cluster).

- Uninstall Cerify on all of the Media Test Units.

Software reinstallation

To reinstall Cerify, you must uninstall Cerify, and then rerun the installer. Rerunning the installer that was used to install the current version of Cerify will cause Cerify to be uninstalled. It does not repair the existing installation.

Software upgrade

To upgrade your existing version of Cerify to the latest version, run the setup file for the latest version of Cerify and follow the on-screen instructions.

NOTE. Dongles used with previous versions of Cerify need to be reprogrammed to be used with version 7.2 or above. If an existing version of Cerify is being upgraded to version 7.2 or above, then it is recommended that users send in their c2v files to Tektronix to obtain a new corresponding v2c file before installing the upgrade. This will allow users to program the dongle with the new v2c file before using Cerify version 7.2 or above.

If you want to upgrade Cerify in an HA cluster installation, the HA dongles on the Supervisor and Secondary Supervisor systems both need to be upgraded.

It is possible to upgrade any type of Cerify installation to any other Cerify installation type (for example, upgrading a Media Test Unit to a Supervisor).

If you would like to back up the current database while you are upgrading from Supervisor, Secondary Supervisor, or Standalone Cerify, choose the **Backup database** option during the upgrade process. The current database is backed up to the location `C:\Documents and Settings\<User name>\Cerify\CerifyConfig_<version>_<timestamp>` by default. You may change this location by choosing a different folder for backing up the files.

The upgrade process also backs up relevant configuration files from the current installation. These files are backed up to `C:\Documents and Settings\<User name>\Cerify\CerifyBackUp_<version>_<timestamp>`.

When you are upgrading to a Supervisor or standalone Cerify, the database is upgraded automatically after the installation. If the database upgrade fails, the installer will install Cerify with a clean database and inform you about the failure. The **Backup database** option will not be available while upgrading from Media Test Unit as they do not have their own database and process the files from the Supervisor's database.

Upgrading a cluster

Insert the installer CD and follow the on-screen instructions. To upgrade a cluster, do the following:

- Upgrade Cerify on the Supervisor by running the latest version of installer and choosing Supervisor as installer type. You can upgrade to either Supervisor for a normal Enterprise cluster or to Supervisor for an HA cluster by choosing the appropriate options.

- Upgrade Cerify on the Secondary Supervisor by running the latest version of installer and choosing Secondary Supervisor as the installer type.

- Upgrade Cerify on all of the Media Test Units by running the latest version of installer and choosing Media Test Unit as the installer type. You can upgrade to either Media Test Unit for a normal Enterprise cluster or to Media Test Unit for an HA cluster by choosing the appropriate options.

Refer to the *Software upgrade* section for instructions on upgrading.

Reverting to the previous version of Cerify

In some circumstances, such as a failed software upgrade, you may wish to revert to an older version of Cerify. To do this, follow these steps:

NOTE. Before proceeding, you should have a database backup and a copy of configuration files from the version you would like to revert to.

1. Uninstall the current version of Cerify. While uninstalling, back up the database by selecting the **Backup database** option.

2. Install the older version of Cerify.

3. Restore the database of older version using the CerifyDatabase Utility tool. For help on how to use this tool, refer to the "Database Backup/Restore Utility" section in the user manual.

Network settings

NOTE. The Cerify software does no particular configuration of any network interfaces - IP address, netmask, DNS, Net BIOS, etc. These should be set using the usual Windows methods.

Two network interfaces

In most circumstances, the PC on which Cerify is installed requires only one network interface. There are three scenarios where it is necessary to have two network interfaces:

■ When the network on which the Web clients will access the Web user interface needs to be physically separate from the network that stores the media file assets.

■ When the Cerify system is to access media files from a Grass Valley Profile or K2 server. In this case, the additional network interface should be connected to the control network that runs the Grass Valley AMP service. This enables Cerify to list the contents available on the Grass Valley servers. The first network interface on the PC should continue to be connected to the video server network as follows:

  − On a standalone Profile XP, to either the Media Ethernet card, if present, or the Ethernet interface of a Universal Interface Module (UIM), if present

  − On a SAN-based Profile XP network, to the Gigabit Media network provided by a Universal Interface Module, if present

  − On a SAN-based K2 network or a standalone K2 Media Client, to the Media/FTP network

  For a K2 network, it is possible to use direct FTP connectivity, in the same fashion as other video servers. In this case, the AMP control network does not need to be accessed and no additional network interface is needed.

■ When installing a Supervisor or Secondary Supervisor for an HA (high availability) cluster. In this case, the second network is used for communication to Cerify via Ceritalk or Web user interface.

Configuring the Cerify installation

See *Appendix E: Configuring Your Cerify Installation* in the *Cerify User Manual* for information about how to configure your Cerify installation for the best performance.

Operation

Getting acquainted

User interface

The user interface consists of a structured collection of pages accessed using a Web browser. The following figure shows the elements that are common to most of the pages in the Cerify Web user interface. The Jobs Monitor page will not contain any jobs when you login to Cerify for the first time after the installation, but will look similar to the following after you perform the tutorial. The elements of the Job Monitor page are shown and described in the following figure and table.

Item		Description
1.	Navigation bar	The navigation bar provides a quick route to the top level of any of the pages.
2.	Auto-Refresh and login details link	Click Auto-Refresh to On to view update progress and job status. The login details, located below the navigation bar at the top-right section of the screen, show who you are logged in as and provide a link enabling you to log out. The license status of Cerify is also reported in this section.
3.	Tables	The system displays a collection of entities in the form of tables. Several types of entities can be created, edited, and displayed, such as Jobs, Profiles, Templates, MediaSets, MediaLocations, and Users. The role of these entities and the relationship between them is explained later in this manual. (See page 16, *Overview*.)
4.	Footer	The footer displays a copyright notice and version information.
5.	Archive/Restore Control	The Archive/Restore control allows you to archive and restore entities.
6.	Active/Archive View Control	The Active/Archive view control allows you to choose which entities of a particular type to view. *NOTE. When an entity is archived, it is not removed from the database, but it becomes inactive. You cannot construct new entities from inactive entities.*
7.	Trail widget	The trail widget allows you to see your position in the hierarchy and navigate from this position.
8.	Icon	The following table lists the icons used in the interface. (See Table 1.)

Table 1: User interface icons

Icon	Description
	Collapse this section
	Expand this section
	Copy this item
	Remove this item
	Edit this item
	Directory
	File in a directory
	Open a context-sensitive help topic
	Status unknown
	Failed with a fatal error status
	Failed with an error status
	Failed with a warning status
	Succeeded with no errors or warnings
	Item created through the Cerify Web user interface
	Item created through CeriTalk API
	Sort items in this column in descending order
	Sort items in this column in ascending order
	Click this button to trigger the selected action
	Adds another set of values to the rules
	Removes any set of values from the rule

Accessing the online help

You can access help topics by clicking **Help** on the Navigation bar or clicking the icon.

Concepts

Users

Before using the system, you must log in with your user name and password credentials. These credentials are assigned by a user who has administrator access.

By default, the system is installed with a single predefined user whose name and password are both set to **admin**. You should change the password after you log in for the first time. Administrator access rights allow you to modify system properties, and in particular to create and modify MediaLocations and Users.

MediaLocations

A MediaLocation is a local or network file storage location from which the system can access media files. Typically, this is a directory on the hard drive or a video server that provides FTP or Windows file share access. To create a MediaLocation, you must supply its URL and the user name and password required to access this URL. In addition, you must supply a unique name to be used within the system to identify the MediaLocation.

Only users with administrator access are able to create or modify MediaLocations.

MediaSets

A MediaSet is a collection of media files that you want to check.

A MediaSet can be a DropBox. A DropBox is a directory that is continually monitored for new media files. A MediaSet that is not a DropBox is simply a static collection of media files manually selected from one or more of the MediaLocations.

If a Job is associated with a DropBox, every file that appears in the DropBox over time will be processed.

Templates

To check a media file, you must define which checks should be applied when the file is tested. A Template is a collection of such checks chosen to perform specific tests required by you. The four types of Templates are:

- ■ Container Templates, which apply to the transport/container layer of a media file
- ■ Video Templates, which apply to the digital video content of a media file
- ■ Audio Templates, which apply to the digital audio content of a media file
- ■ Action Templates, which specify actions to be performed as a result of processing a media file

You can create multiple Templates of the same type for different purposes. For example, you might create a Movies Template, which contains a set of rules appropriate for HD MPEG-2 content, and an on-line content Template, which contains a set of rules appropriate for lower resolution H.264/AVC content.

NOTE. *Some example templates are preloaded onto Cerify. These templates can be used, copied, edited, and archived in the same way as those created by users. The XML files containing these templates can be found in* `<Installation directory>/Example Templates`.

Profiles

A Profile gathers together a container, video, audio, and action Template, providing a complete set of checks that can be applied when you want to test one or more media files. Any of the component Templates can be omitted, depending on your requirements. For example, it makes no sense to apply any container or audio checks to a media file that consists solely of a video elementary stream.

Jobs

A Job is the term given to an individual testing process that can be run by the system. Each Job can process multiple media files or a single media file, depending on your requirement. The set of files processed by a Job is defined by its MediaSet.

By creating a Job, you request the checks defined by a particular Profile be applied to the files in a particular MediaSet. In addition, you must specify the name and priority of the Job. The system can queue multiple Jobs to be run, whereby each Job is scheduled to be processed according to its priority.

The system processes one media file at a time.

How long it takes to process a Job depends upon a number of factors:

- The resolution of the video being processed

- The video standard concerned (some standards, such as H.264/AVC, take more time to process)

- The number of tests selected (performing all the video quality checks can be processor intensive, because it requires the analysis of every pixel in each frame of video)

- The bit rate

- Hardware performance of the PC on which Cerify is installed

Alerts

Alerts announce any checks that fail as a Job executes. Each alert indicates the severity of the failure, as well as where and why the check failed. The system gathers alerts associated with a particular Job, so that you can access the results from the top level and easily navigate to the details, such as which individual frames have Alerts.

The system organizes and summarizes any alerts raised against a particular Job, so that, at the top level, a single processing result status can be assigned to the Job. To view more detailed information, you can drill down through the interface, revealing (for example) which individual frames have raised alerts.

Reports

Reports provide you with a way to query the system database and obtain information in a predefined format. A Job report presents the results of a particular Job in tabular form.

Procedures

Overview

The following figure shows the dependencies between the entities that make up a Job. For example, a MediaLocation must exist to create a MediaSet and a MediaSet must exist to create a Job.

NOTE. A Profile requires at least one type of Template, not necessarily all four types.
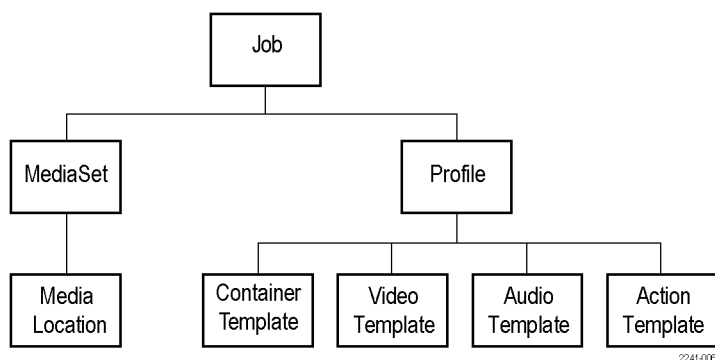
How to start the Cerify application

Perform the following procedure to start the Cerify application.

1. Click the **Start Cerify** icon on the desktop to Launch the Cerify application.

2. Enter your **Username** and the **Password** in the login page. The default Username and Password are admin.

3. Once you are logged in, you can see the Jobs Monitor page.
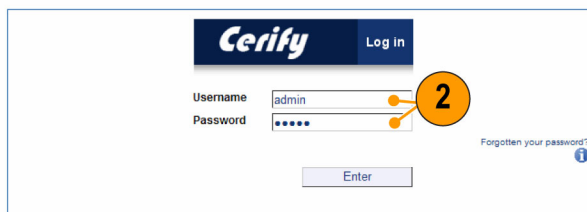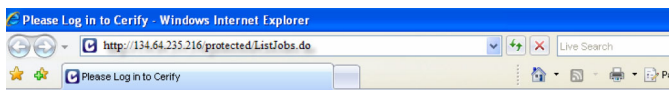
How to start a cluster

Perform the following steps to start a cluster.

1. Start Cerify on Supervisor unit first.

2. Start Cerify on Media Test Units.

3. Enter the URL `http://` `<Cerify host name>` into your Web browser where Cerify host name is Supervisor's host name.

NOTE. By selecting the Media Test Units link on the Admin page, it is possible to view the status of the Media Test Units connected in a cluster. Since a standalone system does not connect to any Media Test Units, this link is unavailable in the Web UI of a standalone system. After clicking the link, you will be taken to the Media Test Units page which lists all the Media Test Units that are in the cluster.

How to create a MediaLocation

You can create and modify MediaLocations only if you have administrator access to Cerify.

1. Click the **Admin** button on the Navigation bar to access the Admin page.
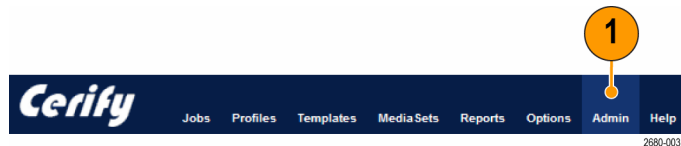
2. In the Cerify Administration page, click the **Go** button to create a new MediaLocation.
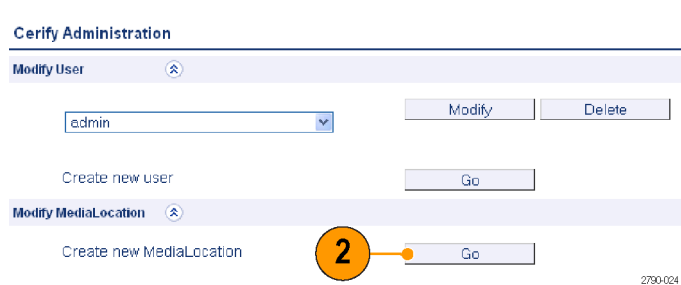
3. In the New MediaLocation page, fill in the fields as follows:

 ■ **MediaLocation Name**: Cerify example content

 ■ **URL**: `c:\Program Files\Tektronix\ Cerify\cerify_demo`

NOTE. The URL used above assumes that you have installed Cerify in the location, C:\Program Files\Tektronix\Cerify.

*NOTE. Leave the **Username** and **Password** fields blank.*

4. Click **Create**.

How to create a MediaSet

Once you have created a MediaLocation, you can create a MediaSet that collects the files at this location.

1. Click the **MediaSets** button on the Navigation bar.

2. In the MediaSets page, click the **New MediaSet** button to create a new MediaSet.

3. In the New MediaSet page, do the following:

 ■ Fill in the **Name** field.

 ■ Set the **DropBox** field to **no**.

4. Click **Create**.

5. In the Edit MediaSet page, you can do the following:

■ Add files to the MediaSet by browsing through the network or by entering the full path of the file in the File name text field at the bottom of the page (the path must include the full URL of the file, for example, `c:\Program Files\Tektronix\ Cerify\cerify_demo\news\ airport_interview.ts`).

NOTE. Only files that exist within folders/sub-folders of an existing MediaLocation can be added to a MediaSet

■ View the contents of a directory by double-clicking the directory icon.

■ Close the directory and go up a level, open the drop-down menu control at the top right of the file browser to provide a selection of recent directories.

■ Select a file by double-clicking the file (📄) icon.

How to create a Template

To test the files in the MediaSet that you have created, you need to decide the checks to apply. You can apply checks to the container or wrapper layer, the video stream, and the audio stream, using container, video, and audio Templates, respectively.

1. Click the **Templates** button on the Navigation bar.

2. In the Templates page, scroll down to view the Video Templates section and click the **New Video Template** button.

3. In the Select Template Type page, do the following:

   ▪ Select the type of Template from the **Please select a type for the template** drop-down menu.

   ▪ Click **Select**.

NOTE. The Template type you choose depends on the type of video content you want to check. This type will be the Video Standard used when the video was encoded, for example, MPEG-2 or H.263.

4. In the **New Template** page, enter a name for the Template.

5. Configure the checks to be applied by selecting the check boxes and entering values into the text fields.

6. Use the ✚ ━ buttons to configure the Resolution rule with multiple sets of valid values. For a full explanation of the checks performed by each rule, click the ⓘ icon next to each rule name.

7. Click the **Create** button at the bottom of the page to create the new Video Template.

NOTE. The new Template will not be saved until you click the Create button at the bottom of the page. When you click Create, the system will check that the fields you have filled contain valid data, and prompt you to fix any problems. If there are no problems, the new Template will be created and stored in the database.

When this MPEG-2 Video Template is used to check a video stream, it will check the following:

■ The video is MPEG-2 encoded.

■ The video is encoded using MPEG-2 Main Profile, Main Level.

■ The video bit stream syntax conforms with the MPEG-2 Standard, but any alerts relating to Buffer analysis and alert number 22209 are suppressed.

■ A maximum of 500 alerts are displayed.

■ Each alert type is displayed a maximum of 20 times.

■ The video resolution is 720 by 480 pixels or 1280 by 1080 pixels.

You can also create an Audio Template and a Container Template similarly.

To create an Audio Template, select **New Audio Template** and select **MPEG-1 / MPEG-2 Audio** as the template type. For the Container Template, select **MPEG-2 Transport Stream** as the Template type.

NOTE. In this example, you will not create an Action Template. If you want to check a different video format, you should select a different codec type in step 3 of the Creating a Template procedure.

How to create a Profile

To use your new Video Template in a Job, you must include it in a Profile.

1. Click the **Profiles** button on the navigation bar.

2680-013
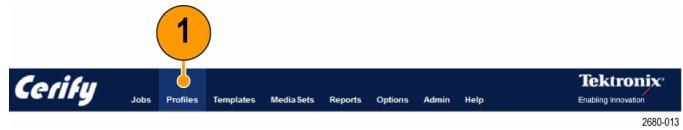
2. In the **Profiles** page, click the **New Profile** button.
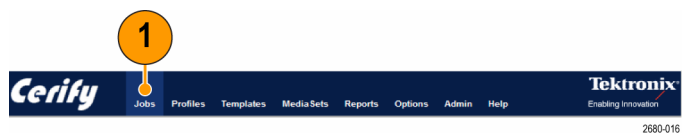

2680-014
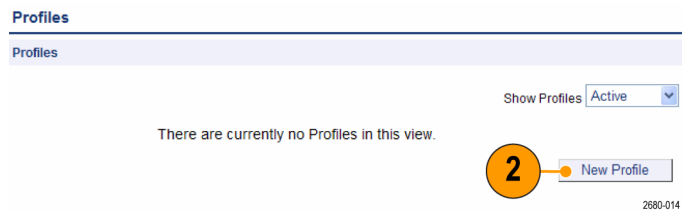
3. In the **New Profile** page, enter a name and a description for the Profile.

4. Select the Templates you have created from the drop-down menu.
   You can select multiple audio templates, if required.

5. Click **Create** to create the Profile.
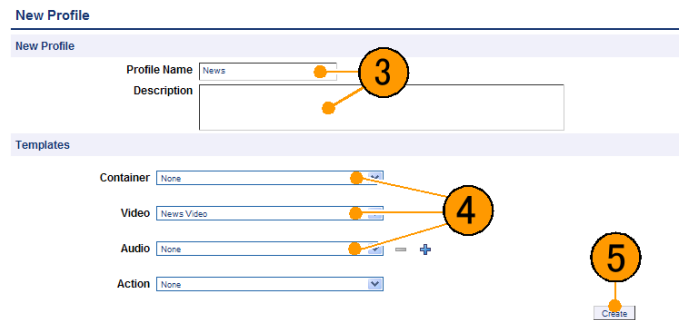
How to create a Job

Once you create a MediaSet and a Profile, you can create a Job.

1. Click the **Jobs** button on the navigation bar.

2680-016

2. Click the **New Job** button.

2680-017

3. In the **New Job** page, do the following:

- Enter a name for the Job.

- Set the Job Priority to Low.

4. Select the Profile and MediaSet that you have created.

5. Click **Create** to create the job.

How to inspect Job results

1. Click the **Jobs** button on the Navigation bar.

2. In the Job Monitor page, click the **AutoRefresh** button in the page header.

3. In the Jobs Monitor page, view the Job results. The ✔ icon indicates that the Job has succeeded.

How to generate a Report

1. Click the **Reports** button on the Navigation bar.
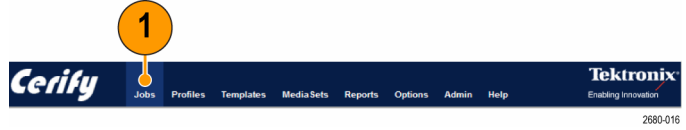
2. In the Reports page, enter the name of the job that you created in the **Enter Jobname** field.

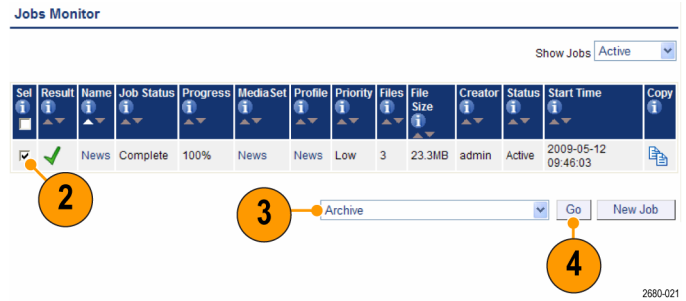**3.** Click the **Generate** button to generate a report of your Job.

How to archive the Job

1. Click **Jobs** on the Navigator bar.

2. In the Job Monitor page, select the Job you want to archive by selecting the check box in the left column of the Jobs Monitor table.

3. Ensure that the action drop-down menu under the table shows Archive.

4. Click **Go** to archive the Job.

5. To view archived Jobs, set **Show Jobs** to Archived.