

Camtasia Relay[®]

Server Security Administrator Guide

Release 1.1

June 2009

© 2009 TechSmith Corporation.
All rights reserved.

Contents

- Introduction.....1
- General Principles.....1
 - Reduce Attack Surface.....1
 - Segregation of Duties1
 - Keep Patches Up-to-Date for All Components.....1
 - Strong Passwords.....2
 - Know Your Servers.....2
- Suggested Workflow for this Guide.....3
- Server Hardening Quick Start Guide4
- Firewall Rules.....5
 - Ports Required by Publishing Destination5
 - Add a Windows Firewall Exception6
 - Conditional Ports6
 - Local SQL Server6
 - Remote SQL Server Ports7
 - Firewall Rules Resources.....7
- Windows Server Hardening8
 - Required Server Roles8
 - Installing the Application Server Role.....8
 - Windows Server 20088
 - Windows Server 2003.....9
 - Security Configuration Wizard9
 - Disable Unnecessary Services9
 - Windows Server Auditing..... 10
- IIS Hardening 11
 - Windows Server 2008 / IIS 8 11
 - Windows Server 2003 / IIS 6 11
 - Configure SSL 13
 - Request a Server Certificate in Windows Server 2008..... 13
 - Request a Server Certificate in Windows Server 2003..... 14
 - Disable Older Versions of SSL and Weak Ciphers..... 14
 - SSL Resources 15
- SQL Server Hardening..... 16
 - Disable Unused SQL Services 16
 - Restrict SQL Server Protocols..... 16
 - Restrict Remote Access 17

Secure Communication Between Relay and SQL.....	17
SSL.....	18
IPSec.....	18
Server Auditing	18
SQL Server Security	19
Resources for SQL Server Hardening.....	19
Configurable Relay Security Features	20
Forgotten Password Policy.....	20
Account Lockout	21
Password Complexity Rules.....	22
LDAP over SSL.....	22
Tools.....	23
Network/Server Security Assessment	23
Known Risks	23
General Server Security Resources	24
Appendix A: SQL Server Security.....	25

Introduction

The purpose of this guide is to help Camtasia Relay administrators securely deploy and manage Camtasia Relay within their organization's network environment. The target audience for this guide is Camtasia Relay administrators who manage the server environment in which Camtasia Relay is hosted but also desire some assistance in making these servers more secure.

This guide provides high-level guidance for hardening Windows Server, IIS, SQL Server, and Camtasia Relay so the environment hosting Camtasia Relay is more secure against attacks. In many cases, the default settings for these components will be appropriate for your organization but this guide should help those administrators who wish to put in the extra effort to further improve their security. Please note that this document is not an extensive guide for hardening your organization's servers against attacks, this guide is only intended to help you get started. Where possible, we provide links to resources to help you further secure the environment where Camtasia Relay is hosted.

Please note that network security is outside the scope of this guide. This document does not provide any guidance on network security issues such as designing a secure network architecture for Camtasia Relay Server(s) (and associated components), network monitoring, or the use of network security appliances such as firewalls, intrusion detection/prevention systems (IDS/IPS), web application firewalls (WAF), etc. This guide is not intended to supersede your organization's network security policies and procedures; it is meant to complement them.

Also note this guide does not discuss several areas of server security such as setting up appropriate access control to the physical machine, auditing policies/log monitoring, and maintaining server backups. Administrators are encouraged to seek out additional resources to accomplish these tasks.

▼ Every organization's network, policies, and business needs are different. Administrators should take care that any configuration changes do not conflict with your organization's business needs, policies, and applicable standards and regulations.

Disclaimer: TECHSMITH CORPORATION MAKES NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED, TO ANY IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS FOR PARTICULAR PURPOSE, TITLE, NONINFRINGEMENT OR AS TO THE ACCURACY OF THE INFORMATION CONTAINED IN THIS GUIDE. IN NO EVENT SHALL TECHSMITH CORPORATION BE LIABLE FOR LOSS OF PROFITS, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF YOUR USE OF THE INFORMATION CONTAINED IN THIS GUIDE. THE ENTIRE RISK OF USING THE INFORMATION CONTAINED IN THIS GUIDE IS WITH YOUR ORGANIZATION.

General Principles

Reduce Attack Surface

The majority of recommendations in this guide deal with disabling (or not installing) services not needed by Camtasia Relay to reduce the attack surface of your Camtasia Relay deployment. Attack surface can be intuitively defined as the number of ways in which an attacker can enter the system and potentially cause damage. The rationale behind reducing attack surface is simple: if a service is not needed then it should be removed or disabled so that an attacker cannot target that service. Removing unneeded services also makes hardening components easier (for example, patch management is simplified as there are fewer services that require patching.)



There are usually multiple ways to adjust the settings for many of the components discussed in this guide. We typically only present one set of steps for changing these settings. Please use whatever method you feel is appropriate to manage configuration settings.

Segregation of Duties

Camtasia Relay should only be deployed on a dedicated server. Other services such as mail, DNS, or other web applications should not be hosted on the server hosting Camtasia Relay. This simplifies configuration and administration. Segregation of duties also helps to ensure that security weaknesses in one service do not lead to compromises of other services hosted on the same server (since those services are instead hosted on other servers.)

Keep Patches Up-to-Date for All Components

Update all components in your network with the most recent patches from their respective vendors, if possible. This includes Windows Server, IIS, SQL server, Camtasia Relay, LDAP server software, email server software, etc. Keeping all components up to date helps ensure that your network is protected against previously discovered-and-fixed vulnerabilities; detailed information and exploit code is widely available for many of these previously discovered-and-fixed vulnerabilities. For many components (for example, Windows Server, SQL Server), automatic updates are available so that the system automatically detects and installs new patches and updates.

Strong Passwords

Many of the components involved in hosting Camtasia Relay (including Windows Server accounts, SQL Server users, and Camtasia Relay accounts) rely on passwords for distinguishing authorized users from everyone else. Attackers commonly attempt to guess passwords to gain access to these systems as an authorized user. These attacks are typically executed using automated scripts that try thousands of passwords including common passwords, dictionary words, and random combinations of characters. One of the best defenses against password guessing attacks is the use strong, or hard-to-guess, passwords. Strong passwords should:

- ▶ Have 8 characters in length or more.
- ▶ Combine letters, numbers, and symbols.
- ▶ Not include words from the dictionary.
- ▶ Be different than your username or account name.
- ▶ Be different than passwords used for other systems.

For more suggestions and information on strong passwords, please see the article: **Strong Passwords and Password Security** at <http://www.microsoft.com/protect/yourself/password/create.mspx>.

Know Your Servers

Security is about risk management and trade-offs; in the case of server hardening, increasing security is about managing the risk of an attacker taking advantage of an enabled service with the trade-off of not being able to use that service if it is disabled. An important prerequisite for server hardening is the detailed knowledge of the purpose of the server, its services, and hosted applications and how these services and applications are used by your organization. With this information, you can make informed and intelligent decisions about how to manage your servers' configurations in order to increase security. In other words, we would like to reiterate that every organization's network, policies, and business needs are different. Server administrators should take care that any configuration changes made do not conflict with your organization's business needs, policies, and applicable standards and regulations.

Suggested Workflow for this Guide

We suggest the following workflow for installing Camtasia Relay and server hardening.

1. **Install Windows Server.** Start with a fresh install to reduce the number of installed services and therefore reduce the server's attack surface.
2. **Install Camtasia Relay Server.** To install the Camtasia Relay Server, you need to install a number of prerequisites. This guide contains suggestions for securely configuring several of these prerequisites.
 - a. **Enable the Application Server Role.** If you are installing the Application Server Role prerequisite, see **Installing the Application Server Role**.
 - b. **Acquire a Server SSL Certificate.** If you are installing the prerequisite SSL certificate see **Configure SSL**.
3. **Server Hardening.** After installing Camtasia Relay, follow the suggestions in this guide to further secure Camtasia Relay's hosting environment. If you are new to managing Camtasia Relay and server security see **Server Hardening Quick Start Guide**. Otherwise we suggest you follow this guide in the presented order, starting with **Firewall Rules** through **Configurable Relay Security Features**.

Server Hardening Quick Start Guide

There is a lot to do when hardening your network and servers against attacks and the amount of work required can be intimidating at first. There are many configuration changes suggested in this guide and many more possible improvements that can be found in other resources.

To help you get started quickly, this section lists the five things, at minimum, you should do to improve the security of Camtasia Relay's environment:

1. **Patch Your Servers.**

Update all components to the latest patch level, especially Windows Server and SQL Server and enable automatic updates if possible.

2. **Use Restrictive Firewall Rules.**

Set Firewall rules to "Deny All" and only open the ports specified in the section "Firewall Rules" for servers hosting Camtasia Relay.

3. **Use and Enforce Strong Passwords.**

Use strong passwords for the Windows Server administrator account, SQL Server users, and Camtasia Relay administrator accounts.

4. **Enable Only the Application Server Role.**

Enable only the Application Server role on any Windows Servers hosting Camtasia Relay. No other roles should be enabled. See **Installing the Application Server Role**.

5. **Use a Valid Server SSL Certificate.**

Obtain a valid server certificate for SSL from a well-known Certificate Authority. See **Configure SSL**.

These five items should help you quickly get started on improving the security of the servers hosting Camtasia Relay. Once you feel comfortable with these five items you can move on to other items in this guide and suggestions from other resources.

Firewall Rules

The following ports are always required for Camtasia Relay to work properly.

Component	Protocol	Ports	Direction
Camtasia Relay Web Application and Service	TCP	80, 443	Incoming
DNS	TCP/UDP	53	Outgoing
NTP	UDP	123	Outgoing

Additional ports may also be required by the operating system or other software (for example, port 1663 for Windows KMS activation.)

Ports Required by Publishing Destination

Depending upon the publishing destinations used by your Camtasia Relay profiles, you may need to open the following ports.

Publishing Destination	Protocol	Ports	Direction
Screencast.com	TCP	80, 443	Outgoing
FTP	TCP	Add the executables "w3wp.exe" and "RelayPublisher.exe" as exceptions. (See below for more details.)	Outgoing
File System	N/A	Check the "File and Printer Sharing" checkbox under Windows Firewall Exceptions.	N/A
File System (Microsoft File Sharing SMB)	TCP/UDP	135-139	Outgoing
File System (Direct-hosted SMB)	TCP/UDP	445	Outgoing
iTunes U	TCP	80,443	Outgoing

FTP Publishing

FTP Publishing requires you to add the following executables as outgoing exceptions to Windows Firewall:

- ▶ **w3wp.exe** (located at C:\WINDOWS\system32\inetrv by default)
- ▶ **RelayPublisher.exe** (located at C:\Program Files\TechSmith\Relay Server\Manager by default)

If configuring a network firewall, the TCP port 21 outgoing and the ephemeral port range (TCP 1024 through 4999 outgoing) should be open for FTP publishing.

Add a Windows Firewall Exception

To access a program through the Windows firewall:

1. In the *Windows Firewall* dialog box, on the **Exceptions** tab, click **Add Program**.
2. Click **Browse**, and navigate to the program executable you wish to access through the firewall, and click **Open**.
3. Click **OK** twice to close the Windows firewall program.

Conditional Ports

Depending upon the configuration of Camtasia Relay and the features enabled, you may need to open the following ports.

Feature	Protocol	Ports	Direction
Email Notification / SMTP	TCP	25 (default SMTP port) or Specified SMTP port	Outgoing
LDAP Authentication	TCP	389 (default LDAP port) or 636 (default LDAP SSL) or Specified LDAP port	Outgoing
Blackboard Notification	TCP	80, 443	Outgoing

- ▶ If email notification is enabled, the SMTP port specified in the SMTP configuration must be open (outgoing) between all Camtasia Relay servers and the designated SMTP server.
- ▶ If LDAP authentication is enabled, the LDAP port specified in LDAP configuration must be open (outgoing) between all Camtasia Relay servers and the designated LDAP server.
- ▶ If Blackboard notification is enabled, then ports 80 and 443 must be open (outgoing) between all Camtasia Relay servers and the designated Blackboard server.

Local SQL Server

You do not need to open ports if Camtasia Relay uses an instance installed on the same machine. However, by default, Camtasia Relay will attempt to connect using TCP/IP and if the appropriate firewall ports are not open (see **Remote SQL Server Ports**) then this connection will fail. To enable Camtasia Relay with restrictive firewall rules, change the Camtasia Relay Server's configuration file `Relay.Manager.exe.config` (located in Camtasia Relay's installation directory, typically `C:\Program Files\TechSmith\Camtasia Relay\Manager\`).

1. Open `Relay.Manager.exe.config` in a text editor.
2. Find the two connection strings for the relay instance. For example,


```
<add name="RelayConnectionString" connectionString="Data Source=<servername>\RELAY; Initial Catalog=Relay; User Id=relay; Password=<password>; Pooling=True;" />
```
3. Change the server name to "(local)" and save the file.

Remote SQL Server Ports

If Camtasia Relay is deployed in a teaming configuration or is configured to use a remote SQL server you must choose to either:

- ▶ list the SQL server executable as an exception to blocked programs or
- ▶ configure the database engine to use a specific TCP/IP port and open this port on servers hosting Camtasia Relay and SQL server.

We recommend listing the SQL server executable as an exception for simplicity.

Use Dynamic Ports / List SQL Server as an Exception

By default, Camtasia Relay uses dynamic ports to access the named 'relay' instance. To continue to use dynamic ports you can list the SQL Server executable (Sqlservr.exe) and SQL Browser as exceptions to the blocked programs on the server hosting the database. Please note that only one instance of SQL Server can be accessed in this way. See **Add a Windows Firewall Exception** to add SQL Server and SQL Browser as exceptions to Windows Firewall rules.

By default, SQL Server (Relay) is located at C:\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL\Binn\Sqlservr.exe and SQL Browser is located at C:\Program Files\Microsoft SQL Server\90\Shared\sqlbrowser.exe. Note that these file paths are dependent on the SQL installation but in most cases the directory structure should be similar. For example, SQL Server (Relay)'s location could change based on the instance identifier in the path (MSSQL.1 in the example above.)

Note that under the Scope tab of the firewall rule, access could be restricted to only allow access from Camtasia Relay servers for increased security.

On the application server hosting Camtasia Relay (not not the SQL Server), it is easiest to create a rule that allows full access to the remote SQL server. When using a named instance, SQL Server binds multiple dynamic ports and it is difficult to create a set of firewall rules that will cover all of the possible ports in order to allow the Camtasia Relay server to communicate with the remote SQL Server. Therefore it is easiest to create a rule to allow the Camtasia Relay Server full outbound access to the remote SQL Server.

Use Static Ports

You may want to use static ports by configuring the database engine to use a specific TCP/IP port and then opening this port on servers hosting Camtasia Relay and SQL server. Please see the following resources for more information on configuring static ports.

- ▶ **How to Configure a Firewall for SQL Server Access:**
[http://msdn.microsoft.com/en-us/library/ms175043\(SQL.90\).aspx](http://msdn.microsoft.com/en-us/library/ms175043(SQL.90).aspx)
- ▶ **How to Configure a Server to Listen on a Specific TCP Port (SQL Server Configuration Manager):**
[http://msdn.microsoft.com/en-us/library/ms177440\(SQL.90\).aspx](http://msdn.microsoft.com/en-us/library/ms177440(SQL.90).aspx)

Firewall Rules Resources

- ▶ **Service overview and network port requirements for the Windows Server system**
<http://support.microsoft.com/kb/832017>
- ▶ **Windows 2003 - Windows Firewall Technical Reference**
<http://technet.microsoft.com/en-us/library/cc779199.aspx>
- ▶ **Windows Firewall Center** <http://technet.microsoft.com/en-us/network/bb545423.aspx>

Windows Server Hardening

Securing the Windows Server operating system is an important part of securing your network. A few steps can reduce the attack surface of Windows Server. After installing Camtasia Relay, you should:

- ▶ Delete or disable unused system accounts.
- ▶ Disable the Windows guest account.
- ▶ Rename the administrator account.
- ▶ Enforce a strong password policy for all accounts. For instructions on how to configure a password policy, please see the article **Enforcing Strong Password Usage throughout Your Organization** at <http://technet.microsoft.com/en-us/library/cc875814.aspx>.

In addition to simple steps, properly configuring the roles and services on the server can further help secure it.

Required Server Roles

When installed on Windows Server 2003/2008, Camtasia Relay requires that the Application Server role be enabled. No other roles are required.

Installing the Application Server Role

Windows Server 2008

Follow the directions for installing the application server role (<http://technet.microsoft.com/en-us/library/cc754684.aspx>) and install only the server role services specified in step number seven below.

To install the Application Server role:

1. Select **Start > Server Manager**.
2. If the *User Account Control* dialog box appears, confirm that the action it displays is what you want, and click **Continue**.
3. On the **Action** menu, select **Add Roles**.
4. The *Add Roles Wizard* appears. Click **Next**.
5. The *Select Server Roles* page appears. Select the **Application Server** check box and click **Next**. If the *Add Features Required for Application Server* dialog appears, click **Add Required Features**.
6. Information about the Application Server role appears. Familiarize yourself with the information, and click **Next**.
7. On the *Select Role Services* page, only install the **Web Server (IIS) support** service role. Other service roles are not required by Camtasia Relay. Select **Web Server (IIS) support** and click **Next**. If the *Add Required Services* dialog appears, verify the services to be added are appropriate and click **Next**.
8. Click **Install** to begin installing the Application Server role with the options that appear on the page. When the installation process is finished, the status of the installation appears on the *Installation Results* page.

Windows Server 2003

Follow the directions for installing the application server role and removing an unneeded service: Microsoft Distributed Transaction Coordinator (DTC) for remote access.

To install the Application Server role:

1. Select **Start > Server Manager**.
2. Click **Add or remove a role**.
3. The *Configure Your Server Wizard* appears. Click **Next**.
4. Select **Application server (IIS, ASP.NET)** and click **Next**.
5. On the *Application Server Options* page, select the **Enable ASP.NET** checkbox. Click **Next**. (Do not check FrontPage Server Extensions.)
6. On the *Summary of Selections* page, click **Next**.
7. The *Windows Components Wizard* will appear. Insert your Windows Server Service Pack 2 CD when prompted.

To disable Microsoft Distributed Transaction Coordinator (DTC) for remote access

1. Click **Start**, and navigate through **Control Panel** to **Administrative Tools** and click **Component Services**.
2. Click **Services**.
3. Double-click **Distributed Transaction Coordinator**.
4. In the Startup type list, click **Disabled**.
5. Click **Stop**, and then click **OK**.

Resources for Installing and Configuring the Application Server Role

- ▶ **Running IIS 6.0 as an Application Server on Windows Server 2003**
<http://technet.microsoft.com/en-us/library/cc756814.aspx>
- ▶ **Installing and Configuring Application Server on Windows Server 2008**
<http://technet.microsoft.com/en-us/library/cc731311.aspx>

Security Configuration Wizard

Disable Unnecessary Services

If you are installing Camtasia Relay on a new installation of Windows Server 2008 then the default services installed for the operating system and the application server role are most likely appropriate for your organization. If you install Camtasia Relay on Windows Server 2003, especially an older installation of Windows Server or alongside other applications (note this both violates the principle of segregation of duties and the Camtasia Relay specifications), then it may be appropriate to disable unneeded services in order to further harden your server.

Use the Security Configuration Wizard to disable unneeded services and further harden Windows Server 2003. Please see the articles (such as the SCW Quick Start Guide) under **Security Configuration Wizard for Windows Server 2003** at <http://www.microsoft.com/windowsserver2003/technologies/security/configwiz/default.mspx>.

The Security Configuration Wizard is also available for Windows Server 2008 and is very similar to the Security Configuration Wizard used for Windows Server 2003.

Windows Server Auditing

It may be useful to monitor successful/failed logons, policy changes, and resource access for the Windows Server hosting Camtasia Relay. You can use the Security Configuration Wizard to choose specific resources to audit. Alternatively, you can use Windows server's Administrative tools to edit the local security policy. Refer to the Windows Server documentation for help using the Security Configuration Wizard.

- ▶ **Security Configuration Wizard for Windows Server 2003**
<http://www.microsoft.com/windowsserver2003/technologies/security/configwiz/default.mspx>
- ▶ **Security Configuration Wizard for Windows Server 2008**
<http://technet.microsoft.com/en-us/library/cc771492.aspx>

IIS Hardening

To access IIS settings for the Camtasia Relay web site: Click **Start** and navigate through **Administrative Tools** and click **Internet information Services (IIS) Manager**.

Windows Server 2008 / IIS 8

Remove Unnecessary HTTP headers

Remove unneeded HTTP headers that may be configured in IIS such as "X-Powered by ASP.NET".

1. In IIS Manager, select the server name on the left.
2. Double click on **HTTP Response Headers**.
3. Select any items listed in the table and click **Remove**.
4. The *HTTP Response Headers* removal confirmation dialog appears. Click **Yes**.

Remove Unnecessary Extensions

1. In IIS Manager, select the server name on the left.
2. Double-click on **Handler Mappings**.
3. Remove any entries in the table with a **Path** value of *.rem, *.soap, *.svc, *.asmx, trace.axd, and WebAdmin.axd as well as the OPTIONS Verb Handler.
 - a. Select the entry you wish to remove.
 - b. Click **Remove**.
 - c. The *Confirm Remove* dialog appears. Click **Yes**.

Remove Unnecessary HTTP Methods

On Windows Server 2008, we consider it unnecessary to remove any HTTP verbs. The HTTP verbs enabled by default should be appropriate.

Windows Server 2003 / IIS 6

Remove Unnecessary HTTP Headers

Remove unneeded HTTP headers that may be configured in IIS such as "X-Powered by ASP.NET".

1. In IIS Manager, right-click on **Web Sites** and click **Properties**.
2. Click the **HTTP Headers** tab.
3. Select any items in the *Custom HTTP headers* box and click **Remove**.
4. You may be prompted to also remove the custom header from child websites. Click **Yes**.

Remove Unnecessary Extensions

Camtasia Relay requires the following application extensions to be enabled: .ashx, .aspx, .axd, .config, .jrpc, and .merge. All other methods can be safely removed.

1. In IIS Manager, click on the plus symbol next to **Web Sites**.
2. Click on the plus symbol next to **Default Web Site**.
3. Right-click on **Relay** and select **Properties**.
4. The *Relay Properties* page appears. Click on the **Virtual Directory** tab.
5. Click on the **Configuration** button on the right side of the page.
6. Remove all extensions *except*: **.ashx**, **.aspx**, **.axd**, **.config**, **.jrpc**, and **.merge**.
 - a. Select the application extension and click **Remove**.
 - b. A confirmation dialog appears. Confirm that the action it displays is what you want, and click **Yes**.

Remove All HTTP Methods Except GET, POST, and HEAD

For all remaining extensions, remove all HTTP methods except GET, POST, and HEAD.

1. In IIS Manager, click on the plus symbol next to **Web Sites**.
2. Click on the plus symbol next to **Default Web Site**.
3. Right-click on **Relay** and select **Properties**.
4. The *Relay Properties* page appears. Click on the **Virtual Directory** tab.
5. Click on the **Configuration** button on the right side of the page.
6. Remove all HTTP methods except GET, POST, and HEAD for the extensions: .ashx, .aspx, .axd, .config, and .merge.
 - a. Select the application extension to change and click **Edit**.
 - b. In the Limit to: text box, remove any words that are not GET, HEAD, POST.
7. Remove all HTTP methods except POST for the extensions: .jrpc.
 - a. Select the application extension .jrpc and click **Edit**.
 - b. In the **Limit to:** text box, remove any words that are not POST.

Restart IIS for changes to take effect

You must restart IIS for the changes you made (removing HTTP headers, removing unnecessary extensions, removing HTTP methods) to take effect.

1. Click **Start** and navigate through **Administrative Tools** and click on **Services**.
2. The *Services* window appears. Find **IIS Admin Service** in the list.
3. Right-click on **IIS Admin Services** and click **Restart**.
4. You are prompted to restart other services (World Wide Web Publishing Services and HTTP SSL). Click **Yes**.

Configure SSL

Camtasia Relay requires SSL in order to protect users' sensitive data in-transit and to provide assurance that users are communicating with the right server. With SSL, all data transmitted to the website is encrypted and integrity-protected. To enable SSL, a valid SSL server certificate is needed.

There are three ways to obtain a server certificate:

- ▶ Purchase a server certificate from a commercial Certificate Authority (CA).
- ▶ Request a server certificate from your organization's internal CA.
- ▶ Create a self-signed server certificate for test purposes. Self-signed certificates should not be used for any purpose other than testing.
 - Using a self-signed certificate will result in users' browsers warning them about visiting the Camtasia Relay web application and in some cases may block them from visiting Camtasia Relay altogether.
 - Using a self-signed certificate opens a web server up to certain network-level (man-in-the-middle or server spoofing) attacks which can result in an attacker gaining access to user data (passwords for example) as well as the ability to modify user requests.

We urge you to use a server certificate well-known Certificate Authority, if possible.

Request a Server Certificate in Windows Server 2008

1. Click **Start** and navigate through **Administrative Tools** and then click **Internet Information Services (IIS) Manager**.
2. In the *Connections* pane, click on server name.
3. In *Features View* of the Relay site, double-click **Server Certificates**. See the Microsoft article *Configuring Server Certificates in IIS 7.0* (<http://technet.microsoft.com/en-us/library/cc732230.aspx>) for further instructions on obtaining, installing, and managing server certificates.

Bind a Server Certificate to the Relay Web Site in Windows Server 2008

1. In IIS Manager, click on the plus symbol next to server name.
2. Click on the plus symbol next to **Sites**.
3. Click on **Default Web Site**.
4. Click on **Bindings...**
5. The *Site Bindings* page appears. Click **Add**.
6. The *Add Site Binding* page appears. Select **https** from the dropdown menu.
7. Select the server certificate to add to the Relay web site from the **SSL certificate** dropdown menu.
8. Click **View** to view the server certificate. Review the certificate information to ensure the certificate is valid and the information is correct. Click **OK** when you are finished reviewing the certificate.
9. Click **OK**.

Request a Server Certificate in Windows Server 2003

To request a certificate in the first two situations, use the Web Server Certificate Wizard.

1. Click **Start** and navigate through **Administrative Tools** and then click **Internet Information Services (IIS) Manager**.
2. Click on the plus symbol next to **Web Sites**.
3. Right-click on **Default Web Site** and click **Properties**.
4. The *Default Web Site Properties* page appears. Click the **Directory Security** tab.
5. Click the **Server Certificate** button.
6. The *Web Server Certificate Wizard* appears. Using the Web Server Certificate Wizard you can request a server certificate from your organization's internal CA or from a commercial CA.

See Microsoft's article *Certificates_IIS_SP1_Ops* (<http://technet.microsoft.com/en-us/library/cc757474.aspx>) article for further instructions on obtaining, installing, and managing server certificates.

Bind a Server Certificate to the Relay Web Site in Windows Server 2003

1. In IIS Manager, click on the plus symbol next to the server name.
2. Click on the plus symbol next to **Web Sites**.
3. Right-click on **Default Web Site** and click **Properties**.
4. Click on the **Directory Security** tab.
5. Click on the **Server Certificate** button.
6. The *Web Server Certificate Wizard* appears. Click **Next**.
7. Select the **Assign an existing certificate** radio button. Click **Next**.
8. Select the server certificate to install and click **Next**.
9. Review the certificate information to ensure the certificate is valid and the information is correct. Click **Next** when you are finished reviewing the certificate.
10. Click **Finish**.

Disable Older Versions of SSL and Weak Ciphers

Older versions of the SSL protocol have well-known vulnerabilities and should no longer be used. Certain ciphers, used to perform encryption, are also no longer considered secure and should not be used.

On Windows Server 2008, both SSLv2 and PCT 1.0 are disabled by default. Furthermore the ciphers enabled by default on Windows Server 2008 are appropriate.

Windows Server 2008 SSL Ciphers: <http://technet.microsoft.com/en-us/library/cc766285.aspx>

On Windows Server 2003, both older versions of SSL and certain ciphers should be disabled by following the directions below.

Disable SSLv2 and PCT 1.0 on Windows Server 2003 / IIS 6

1. Click **Start**, click **Run**, type **regedt32**, and click **OK**.
2. In Registry Editor, locate the following registry keys:
 - HKey_Local_Machine\System\CurrentControlSet\Control\SecurityProviders\CHANNEL\Protocols\PCT 1.0\Server
 - HKey_Local_Machine\System\CurrentControlSet\Control\SecurityProviders\CHANNEL\Protocols\SSL 2.0\Server
3. For each key, do the following:
 - a. On the **Edit** menu, select **New > DWORD Value**.
 - b. In the *Value Name* box, type **Enabled**, and then press **Enter**.
 - c. Double-click the value to edit its current value.
 - d. Type **00000000** in Hexadecimal Editor to set the value of the new key equal to "0".
 - e. Click **OK**. Restart the computer.

Resource: <http://support.microsoft.com/kb/187498/en-us>

Disable Weak Ciphers on Windows Server 2003 / IIS 6

1. Click **Start**, click **Run**, type **regedt32**, and click **OK**.
2. In Registry Editor, locate the following registry keys:
 - HKey_Local_Machine\System\CurrentControlSet\Control\SecurityProviders\CHANNEL\Ciphers\RC2 40/128
 - HKey_Local_Machine\System\CurrentControlSet\Control\SecurityProviders\CHANNEL\Ciphers\RC4 40/128
3. For each key, do the following:
 - a. On the **Edit** menu, click **New > DWORD Value**.
 - b. In the *Value Name* box, type **Enabled**, and then press **Enter**.
 - c. Double-click the value to edit its current value.
 - d. Type **00000000** in Hexadecimal Editor to set the value of the new key equal to "0".
 - e. Click **OK**. Restart the computer.

Resource: <http://support.microsoft.com/kb/245030>

SSL Resources

- ▶ **Configuring Server Certificates in IIS 6.0**
<http://technet.microsoft.com/en-us/library/cc757474.aspx>
- ▶ **Configuring Server Certificates in IIS 7.0**
<http://technet.microsoft.com/en-us/library/cc732230.aspx>
- ▶ **TechSmith Support Center: How can I create a self signed SSL certificate for use with Relay?**
http://techsmith.custhelp.com/cgi-bin/techsmith.cfg/php/enduser/std_adp.php?p_faqid=1999
- ▶ **SSLDigger (<http://www.foundstone.com/us/resources/proddesc/ssldigger.htm>)**
You can use this freely available tool to check your server for weak SSL ciphers and to determine if you have older versions of SSL installed.
- ▶ **Microsoft SSLDiagnostics**
(<http://www.microsoft.com/DownLoads/details.aspx?FamilyID=cabea1d0-5a10-41bc-83d4-06c814265282&displaylang=en>) You can use this freely available tool to help diagnose problems with your SSL configuration on Windows Server 2003.

SQL Server Hardening

Hardening the SQL database server helps ensure that your users' data is protected from attackers. Similar to securing Windows Server, several simple steps can help reduce the attack surface of SQL server. You should:

- ▶ Delete or disable unused system accounts.
- ▶ Disable the Windows guest account.
- ▶ Rename the administrator account.
- ▶ Enforce a strong password policy for all accounts.
- ▶ Ensure that SQL Server is using the most up to date Service Pack and patches. (Camtasia Relay expects SQL Server Express 2005 Service Pack 3 or later.)

Disable Unused SQL Services

The services **SQL Server (Relay)** and **SQL Server Browser** are needed. On a new install of SQL Server these should be the only services installed. If you configure Camtasia Relay to use a SQL Server that has other SQL services enabled and these services are no longer needed, then you may wish to disable them.

If SQL Server is hosted on Windows Server 2003 then you should also disable the Microsoft Distributed Transaction Coordinator (DTC) service. See the instructions "**Disable Microsoft Distributed Transaction Coordinator (DTC)**" under the section **Windows Server Hardening**.

Restrict SQL Server Protocols

Restricting what protocols can be used to access SQL server reduces the attack surface the database.

1. Click **Start** and navigate to the **Microsoft SQL Server** program group, through **Configuration Tools** to click on **SQL Server Configuration Manager**.
2. Expand **SQL Server 2005 Network Configuration** and click on **Protocols for RELAY**.
3. Disable SQL Server Protocols for RELAY:
 - a. **Remote SQL Server Deployment:** Make sure that TCP/IP and Shared Memory are the only SQL Server protocols that are enabled. Right click on the protocols you wish to enable and click **Enable**; right click on any protocols you wish to disable and click **Disable**.
 - b. **Local SQL Server Deployment:** Make sure that Shared Memory is the only SQL Server protocol enabled.
4. Expand **SQL Native Client Configuration** and click on **Client Protocols**.
5. Disable Client Protocols:
 - a. **Remote SQL Server Deployment:** Make sure that TCP/IP and Shared Memory are the only SQL Server protocols that are enabled.
 - b. **Local SQL Server Deployment:** Make sure that Shared Memory is the only SQL Server protocol enabled.

Restrict Remote Access

Restrict Remote Logons

Use the Local Security Policy tool to remove the "Access this computer from the network" user right from the Everyone group to restrict who can log on to the server remotely.

1. Click **Start** and navigate through **Administrative Tools** and then click **Local Security Policy**.
2. Click on the plus symbol next to **Local Policies**.
3. Click on **User Rights Assignment**.
4. Double-click on the **Access this computer from the network** entry in the list.
5. The *Access this computer from the network Properties* page appears. Select **Everyone** from the list and click **Remove**.
6. Click **OK**.

Disable Null Sessions (Anonymous Logons)

Null sessions allow for anonymous access which can allow an attacker to connect to your server without authentication.

Restrict null sessions by setting RestrictAnonymous=1 in the registry at the following location.

```
HKLM\System\CurrentControlSet\Control\LSA\RestrictAnonymous=1
```

Secure Communication Between Relay and SQL

You may need to take steps to protect the communication between Camtasia Relay and a remote SQL server (such as when using Camtasia Relay's teaming features.) The communication should either be encrypted (for example, by using SSL or IPSec) or the remote SQL server should be deployed such that attackers cannot intercept traffic to and from the SQL server.

In the case of deploying the SQL server such that attackers cannot intercept traffic to and from the SQL server, the Camtasia Relay Server should be deployed in a demilitarized zone (DMZ) in your network and this DMZ should be physically or logically segmented from the internal network by a stateful packet inspection (SPI) firewall or other network security device. The point-to-point communication between any Camtasia Relay Servers and the remote SQL server should not be across any public network. The remote SQL server should be placed in a more secure portion of your network than the DMZ and should not be publicly accessible, if possible.

In the case of using SSL or IPSec to encrypt Camtasia Relay's communication with a remote SQL server, the following instructions should help you get started.

SSL

1. **Obtain a valid SSL Certificate for SQL Server.** See **Configure SSL** for more information on how to obtain and configure a server certificate. In order for SQL server to use the SSL certificate it must meet certain requirements, which are listed here:
[http://technet.microsoft.com/en-us/library/ms189067\(SQL.90\).aspx](http://technet.microsoft.com/en-us/library/ms189067(SQL.90).aspx).
2. **Configure SQL Server to use the SSL certificate.**
 - a. Before SQL Server can be configured to use the SSL certificate, the account used to run the SQL Server service must be given permission to access the SSL certificate. This account is typically the 'NetworkService' account. Microsoft's freely available WinHttpCertCfg tool can be used to grant the NetworkService access to the certificate. Please note that this tool must be used with the same Windows account used to install the certificate. For information on using the WinHttpCertCfg tool see the following resources:
 - i. [http://msdn.microsoft.com/en-us/library/aa384088\(VS.85\).aspx](http://msdn.microsoft.com/en-us/library/aa384088(VS.85).aspx)
 - ii. <http://blogs.technet.com/mscom/archive/2007/05/30/how-to-get-sql-to-accept-the-cert-or-a-day-or-two-in-the-life-of-an-mscom-debug-engineer-part-2.aspx>
 - b. Once the certificate has been installed in server's certificate store and the SQL server service's account has access to the certificate, SQL can be configured to use this certificate. See the instructions here on how to configure SQL to SSL: [http://technet.microsoft.com/en-us/library/ms189067\(SQL.90\).aspx](http://technet.microsoft.com/en-us/library/ms189067(SQL.90).aspx). Alternatively:
 - i. Click Start, in the Microsoft SQL Server 2005 program group, point to Configuration Tools, and then click SQL Server Configuration Manager.
 - ii. Click the plus symbol next to **SQL Server 2005 Network Configuration**.
 - iii. Right click on **Protocols for RELAY** and select **Properties**.
 - iv. On the **Certificate** tab, select the appropriate SSL certificate.
 - v. On the **Flags** tab, select **Force Encryption: Yes**.
 - vi. Click OK.

IPSec

Alternatively, IPSec may be used to encrypt communication between Camtasia Relay and a remote SQL server. It should be noted though that configuring and deploying IPSec may be considered much more complicated and heavily dependent upon your organization's network architecture. The following resources may help you configure IPSec.

- ▶ **IPSec Overview:** <http://technet.microsoft.com/en-us/network/bb531150.aspx>
- ▶ **Data Access Security – Secure Communication:** http://msdn.microsoft.com/en-us/library/aa302392.aspx#secnetch12_securecommunication
- ▶ **How To: Use IPSec to Provide Secure Communication Between Two Servers:** <http://msdn.microsoft.com/en-us/library/aa302413.aspx>
- ▶ **Using IPSec for Network Protection:** <http://technet.microsoft.com/en-us/library/cc512617.aspx>

Server Auditing

It may be useful to monitor successful/failed logons, policy changes, and resource access for the Windows Server hosting your SQL server. See **Windows Server Auditing** for instructions on setting up auditing.

SQL Server Security

You can change or verify many advanced settings to increase the security of SQL Server. The default settings created by the Camtasia Relay installer are appropriate in many cases. However, if you (1) are using a remote SQL database with Camtasia Relay and (2) the remote SQL Server used by Camtasia Relay has other database instances installed (in the past or currently), and (3) you are comfortable using SQL Server Manager to manage SQL server configuration settings, then it may be appropriate to further secure SQL server using these advanced settings. If so, see **Appendix A: SQL Server Security** for suggestions on securely configuring SQL server.

Resources for SQL Server Hardening


Security Considerations for SQL Server: <http://msdn.microsoft.com/en-us/library/ms161948.aspx>

Configurable Relay Security Features

Camtasia Relay includes several features you can configure to increase the security of Camtasia Relay user accounts.

Forgotten Password Policy

You can allow users managed by Camtasia Relay to change their password if they forgot their password.

 Enabling this feature increases the attack surface of Camtasia Relay.

When this feature is enabled, users managed by Camtasia Relay can submit a CAPTCHA-protected form to request that a unique link be sent to the email address stored for their account. This unique link is active for a short amount of time; this duration is configured by the Camtasia Relay administrator using the User Account Security Settings at `~/Relay/AccountSecurity.aspx`. The forgotten-password link leads to a second CAPTCHA-protected form that users can use to change their password.

An attacker may attack this feature by attempting to guess the unique link and if successful, changing a user's password. Therefore the form employs a number of defenses. CAPTCHA should help to prevent brute-force guessing. The link's short duration also limits the number of guesses an attacker can possibly try during the link's lifetime. Lastly, the password change form reports the same results for valid links and invalid links.

To help prevent an attacker from using Camtasia Relay to send unwanted email to users, the forgotten password feature restricts how often a forgotten password email will be sent to users. If a user (or attacker) requests a forgotten password email for a user and the link from this email is not successfully used to change the user's password then Camtasia Relay will not send the user another forgotten password email for an admin-specified time.

Account Lockout

To prevent an attacker from using a brute-force attack to guess users' passwords, you can enable account lockout. With account lockout enabled, both users managed by Camtasia Relay and users who authenticate via LDAP can be locked out of Camtasia Relay after a number of failed login attempts.

Note that account lockout applies equally to presenters and administrators, including the "relayadmin" account. If your organization intends to use account lockout then additional Camtasia Relay administrator accounts should be created to help prevent a denial-of-service attack against administrators. In a denial-of-service lockout attack, an attacker would use a script to continually attempt to login as an administrator account with bad passwords, causing the account to be locked out so that Camtasia Relay administrators could never log in to that account.

Also note there is not currently a way for administrators to unlock user accounts using the web application. Users must either wait for admin-specified duration for their account to be unlocked or if the "Enable CAPTCHA to unlock" option is enabled, the user can unlock their account and login if they successfully complete the CAPTCHA challenge and provide the correct username and password.

There are a number of settings that must be configured for account lockout.

Setting	Description
Lock account after _____ failed login attempts	Determines how many times a user can attempt to login within a short time period (also specified by the administrator) before their account is locked.
Lock account for _____ minutes	Determines how long a user's account will be locked. After this time period has passed the user will be able to log-in (by providing the correct password) assuming that the user does not fail to log-in again (by providing an incorrect password) within the short time period which may result in the user's account being locked again. If the forgotten password feature is enabled, a user's account will be unlocked when a user changes their forgotten password using the feature.
Reset login attempts after _____ minutes	Determines the short time period in which a number failed login attempts will lock out a user.
Enable CAPTCHA to unlock	If checked, then if a user attempts to log-in to the website using a locked out account, they will be redirected to a CAPTCHA-protected log-in form. If a user provides the correct username, password, and solution to the CAPTCHA challenge, their account will be unlocked and the user will be logged in.

Password Complexity Rules

If password complexity rules are enabled then users managed by Camtasia Relay will be required to provide strong passwords. It is very important to enable this feature to help protect Camtasia Relay users against password guessing attacks. If this feature is not enabled then user passwords are not subjected to any standard of quality.

Please note that users who have set their password prior to enabling this feature may have passwords that do not meet the password complexity rules. Camtasia Relay currently does not warn users or force a password change if their current password does not meet the standard of the password complexity rules. Also note that passwords set for users by an administrator are not subject to password complexity rules. It is the administrator's responsibility to ensure that any administrator-set user passwords are strong passwords.

Password complexity rules are enforced when a logged-in presenter changes their password using the Camtasia Relay web application. If the forgotten password feature is enabled then password complexity rules are also enforced when a user changes their forgotten password using the unique link.

LDAP over SSL

If your organization's LDAP server is deployed in such a way that an attacker may intercept the traffic between Camtasia Relay and the LDAP server then SSL should be used to protect LDAP communications. In this case, SSL is needed to protect the master LDAP user credentials stored and used by Camtasia Relay, as well as the credentials of users that authenticate using LDAP, as they are transmitted to the LDAP server.

During LDAP configuration, check the **Use secure authentication (SSL)** option.

For convenience and testing purposes, Camtasia Relay's LDAP integration feature also offers the ability to "Trust all certificates". Only select this option for testing purposes (for example, when using a self-signed server certificate when you are unable to or do not wish to add the self-signed certificate to the trusted certificate store.) If possible a valid server certificate should be obtained from a well-known Certificate Authority. See **Configure SSL** for more information on how to obtain and configure a server certificate.

Tools

Network/Server Security Assessment

Administrators should regularly run network security assessment tools such as Nessus, Nikto, and Nmap against their servers to identify known vulnerabilities. These tools aren't perfect but they are freely available (and attackers **will** be running them against your server.) Because these vulnerabilities are publicly known and can be easily identified using these tools, it is especially important to patch your servers and protect against these vulnerabilities. Of course, these tools cannot replace the security assessment of a network security specialist but they should help administrators identify and eliminate *some* well-known vulnerabilities.

- ▶ <http://www.nessus.org/download/>
- ▶ <http://www.cirt.net/nikto2>
- ▶ <http://nmap.org/>

Known Risks

 **Camtasia Relay Recorder defaults to ignoring invalid SSL certificates if there is a problem with the Camtasia Relay Server's SSL certificate.**

When connecting to the Camtasia Relay Server, the Camtasia Relay Recorder will attempt to validate the SSL certificate provided by the server. If the SSL certificate is invalid (expired, incorrect name, untrusted Certificate Authority, etc.) then the Camtasia Relay Recorder will ignore the invalid certificate and connect to the server anyways. The user is not alerted that the SSL certificate is invalid in any way. The ability for users to view and to choose whether or not to accept invalid certificates is planned for a future version of the Camtasia Relay Recorder.

If an attacker were to set up a man-in-the-middle attack in your organization's network then the attacker will be able to read SSL traffic (e.g. the user's username and password) that passes through the attacker's server. In this case, the Uploader sets a SSL connection with the attacker, and the attacker establishes another SSL connection with the Camtasia Relay Server. To do this the attacker needs to play "network games" (ARP, DHCP, DNS spoofing) in order to direct the Uploader traffic to the attacker's machine. You should carefully monitor your network for such spoofing attacks.

General Server Security Resources

- ▶ **Windows Server 2003**
<http://technet.microsoft.com/en-us/library/cc706993.aspx>
- ▶ **Windows Server 2008**
<http://technet.microsoft.com/en-us/library/dd349801.aspx>
- ▶ **Windows Server 2003 Security Guide**
<http://www.microsoft.com/downloads/details.aspx?FamilyID=8a2643c1-0685-4d89-b655-521ea6c7b4db&DisplayLang=en>
- ▶ **Windows Server 2008 Security Guide**
 - <http://technet.microsoft.com/en-us/library/cc264463.aspx>
 - <http://www.microsoft.com/downloads/details.aspx?familyid=FB8B981F-227C-4AF6-A44B-B115696A80AC&displaylang=en>
- ▶ **Windows Server 2003 Security Compliance Management Toolkit**
<http://technet.microsoft.com/en-us/library/cc163140.aspx>
- ▶ **Windows Server 2008 Security Compliance Management Toolkit**
<http://technet.microsoft.com/en-us/library/cc514539.aspx>

Appendix A: SQL Server Security

You can change or very many advanced settings to increase the security of SQL Server. The default settings created by the Camtasia Relay installer are appropriate in many cases. However, if you (1) are using a remote SQL database with Camtasia Relay and (2) the remote SQL Server used by Camtasia Relay has had other databases installed in the past or currently, and (3) you are comfortable using SQL Server Manager to manage SQL server configuration settings, then it may be appropriate to further secure SQL server using these advanced settings.

The settings below are typically accessed using SQL Server Manager.

SQL Authentication

Camtasia Relay requires SQL authentication be enabled in order to connect to a remote SQL server. Many resources on securing SQL server may advise you to disable SQL authentication; do **not** disable SQL authentication as Camtasia Relay will no longer be able to connect to the remote SQL server.

Delete or Disabled Unused SQL Users

Unused accounts should be deleted to prevent an attacker using them and their privileges in the event that the attacker gains access to the server.

Relay uses the SQL users “relay”. All other SQL Users should be deleted or disabled from the Relay instance with the exception of the following default required users: “dbo”, “guest”, “sys”, and “INFORMATION_SCHEMA”.

Least Privilege SQL User

The Camtasia Relay SQL user “relay” requires the following SQL service privileges: **datareader** and **datawriter**. No other permissions should be granted. The Camtasia Relay installer should configure the SQL server with least privilege but you should verify that the SQL user has only the privileges listed above and no other.

Use a Strong sa (System Administrator) password

The default system administrator (sa) account has been the subject of countless attacks. It is the default member of the SQL Server administration fixed server role **sysadmin**. Make sure you use a strong password for this account.

Do not grant permissions for the public role

All databases contain a public database role. Every other user, group, and role is a member of the public role. You cannot remove members of the public role. Instead, do not grant the permissions for the public role that grant access to your application's database tables, stored procedures, and other objects. Otherwise, you cannot get the authorization that you want using user-defined database roles because the public role grants default permissions for users in a database.

Remove the sample databases

Any sample databases, if present, (for example, Pubs and Northwind) should be removed using SQL Server Manager.