Product:	OpenText Content Server
Version:	10.5, 16.0.x
Task/Topic:	Security, Deployment, Administration
Audience:	Administrators
Platform:	All
Document ID:	500285
Updated:	December 5, 2016

Best Practices

Content Server Application Security Hardening Guide

Contents

Revision and Release History

Revision	Author(s)	Date
1.0	Tim McCrabb, Technical Lead – Product Security	November 13th, 2015
1.1	Adrienne Farrell, Security Advocate – Content Server	August 4, 2016

Introduction

Every organization should analyze their security requirements and risk tolerance in order to define the requirements for their Content Server implementation. This document is a guide to security hardening Content Server—making the deployment more resilient to attack. It will help administrators to decide which configuration options they should choose in order to meet the needs of business users.

It is important to remember that Content Server works in conjunction with other infrastructure service software (for example: databases, server operating systems, and web servers). This document focuses on the configuration of the Content Server platform only. The configuration of supporting software, services, and servers should be reviewed to ensure that Content Server security is supported by secure supporting systems.

This document defines the options that are part of Content Server 10.5.0 and Content Server 16.0.

NOTE: This document covers releases of Content Server 10.5 up to and including SP1 Update 2016-12, and covers releases of Content Server 16 up to and including 16.0.2.

For Content Server 10.0.0, refer to the:

OpenText Content Server 10.0.0 - Application Hardening Guide

This document includes the default configurations for each configurable item. It is important to note that systems upgraded from previous versions of Content Server will retain the configuration values from the previous version.

Content Server Administrators should review this document and make note of any security features that they wish to implement in order to secure their Content Server deployment according to their organization's policies.

Each security setting item in the document is accompanied by corresponding tag. These tags are intended to help administrators decide which server configuration items they want to implement.

XSS	Cross-site Scripting attack mitigation
CSRF	Cross-site Reference Forgery attack mitigation
SQL	SQL Injection attack mitigation
AUTHENT	Mechanism strengthens user authentication
ASR	Attack surface reduction technique - reduces the exposure of privileged areas of the application
PRIVACY	Affects the privacy of users and/or content
EXTERNAL	Affects security outside the context of Content Server, for instance, settings that exist to comply with security policies

Content Server Updates

Once Content Server is installed it is essential that all of the latest upgrades and patches are applied. It is recommended that you use OpenText Cluster Management to apply the appropriate upgrades/patches.

All upgrades and patches should also be applied for any other OpenText software deployed as part of the Content Server system.

Content Server Configuration

Network Isolation and the Secure Extranet Architecture (SEA)

To support network isolation, Open Text offers Secure Extranet Architecture (SEA) functionality which provides an additional level of security between a potential attacker and Content Server.

The aim of SEA is to minimize the risk of potential attacks on the components of a Content Server system by making effective use of network isolation by controlling end-user access to different network areas/tiers. SEA enables the application server to reside on a different machine and allow secure access to Content Server from an extranet environment (i.e. the Internet). This is achieved by configuring an application server within the DMZ which is separate from the Content Server system that resides in the protected, trusted environment. This means that there is no direct access to the database, the external file store, the Admin server, and the Content Server index from the Demilitarized Zone (DMZ). Only a single port (with well-defined source and destination IP addresses) needs to be opened in the firewall to the trusted backend, and this access uses a proprietary Content Server protocol for communication.

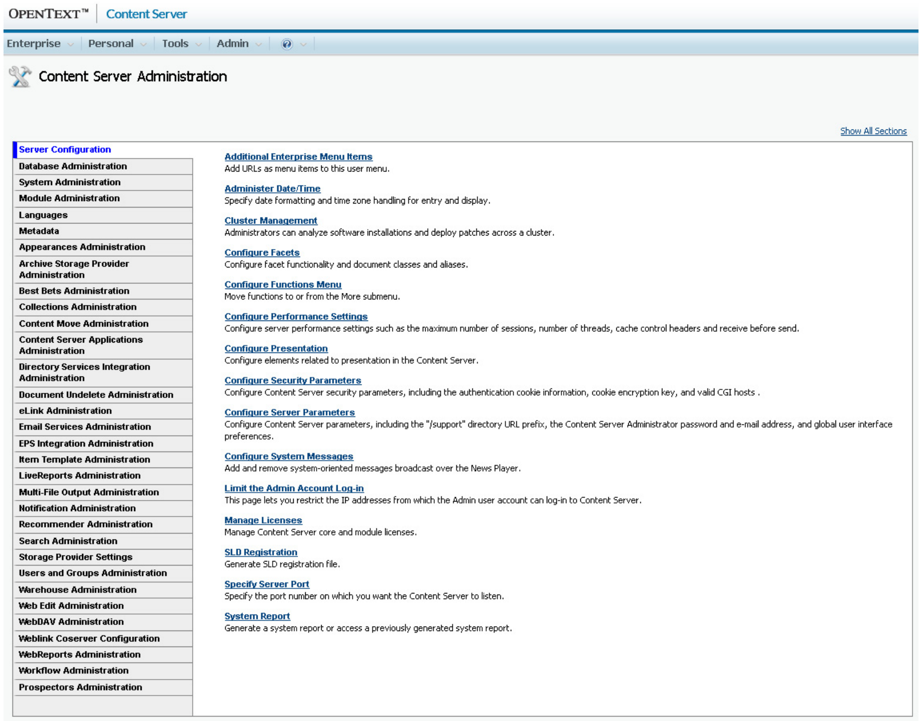
Such extensive use of network isolation and multilayered protection models provides additional protection against buffer overflow attacks and attacks targeting individual weaknesses of the systems in use. An attacker needs to successfully penetrate all layers in such a configuration, which will, according to documented best practices, consist of different types of operating systems and dedicated application servers, specially hardened and continuously monitored in this environment.

Administration Pages

The majority of settings discussed in this user guide can be accessed from the Content Server Administration pages or through direct manipulation of the `opentext.ini` file.

The Content Server Administration pages can be accessed by visiting the link below:

http://server_name/OTCS/cs.exe?func=admin.index


OPENTEXT™
Content Server
Enterprise
Personal
Tools
Admin
Content Server Administration
Show All Sections
Server Configuration
Database Administration
System Administration
Module Administration
Languages
Metadata
Appearances Administration
Archive Storage Provider Administration
Best Bets Administration
Collections Administration
Content Move Administration
Content Server Applications Administration
Directory Services Integration Administration
Document Undelete Administration
eLink Administration
Email Services Administration
EPS Integration Administration
Item Template Administration
LiveReports Administration
Multi-File Output Administration
Notification Administration
Recommender Administration
Search Administration
Storage Provider Settings
Users and Groups Administration
Warehouse Administration
Web Edit Administration
WebDAV Administration
Weblink Coserver Configuration
WebReports Administration
Workflow Administration
Prospectors Administration

Additional Enterprise Menu Items
Add URLs as menu items to this user menu.

Administer Date/Time
Specify date formatting and time zone handling for entry and display.

Cluster Management
Administrators can analyze software installations and deploy patches across a cluster.

Configure Facets
Configure facet functionality and document classes and aliases.

Configure Functions Menu
Move functions to or from the More submenu.

Configure Performance Settings
Configure server performance settings such as the maximum number of sessions, number of threads, cache control headers and receive before send.

Configure Presentation
Configure elements related to presentation in the Content Server.

Configure Security Parameters
Configure Content Server security parameters, including the authentication cookie information, cookie encryption key, and valid CGI hosts .

Configure Server Parameters
Configure Content Server parameters, including the "/support" directory URL prefix, the Content Server Administrator password and e-mail address, and global user interface preferences.

Configure System Messages
Add and remove system-oriented messages broadcast over the News Player.

Limit the Admin Account Log-in
This page lets you restrict the IP addresses from which the Admin user account can log-in to Content Server.

Manage Licenses
Manage Content Server core and module licenses.

SLD Registration
Generate SLD registration file.

Specify Server Port
Specify the port number on which you want the Content Server to listen.

System Report
Generate a system report or access a previously generated system report.

Figure 1

NOTE: Individual deployments may require modification of the `server_name/OTCS/` portion of the link.

Some settings are applied directly through the `opentext.ini` file, which is the main Content Server configuration file. The `opentext.ini` file is a text-based configuration file containing configuration values in the format of name value pairs. The file is located in the `config` directory that is located beneath the Content Server installation directory.

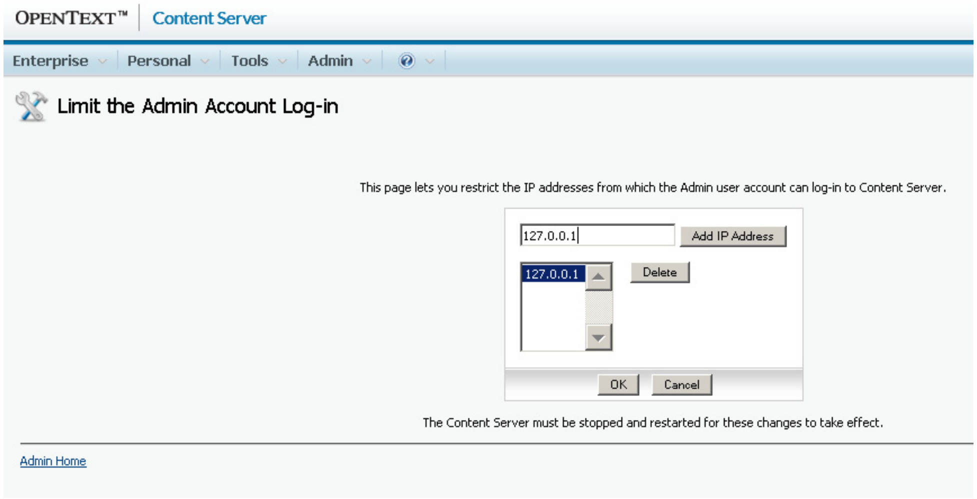
Limiting Access to the Administration Pages

ASR

Content Server Administration → Server Configuration → Limit the Admin Account Log-in

This is a key security setting that limits the access of the Admin user account to selected computers. Its use should be evaluated carefully.

This setting limits the IP addresses from which the **main administration account** (Admin) and the **Administration Pages Password** can be used. This setting should be set to a list of trusted IP addresses that core Content Server administrators use to access the administration pages of Content Server. This will prevent access to administration pages from computers with IP addresses other than those listed, helping to prevent attacks against the administration pages.



Limit the Admin Account Log-in

This page lets you restrict the IP addresses from which the Admin user account can log-in to Content Server.

127.0.0.1

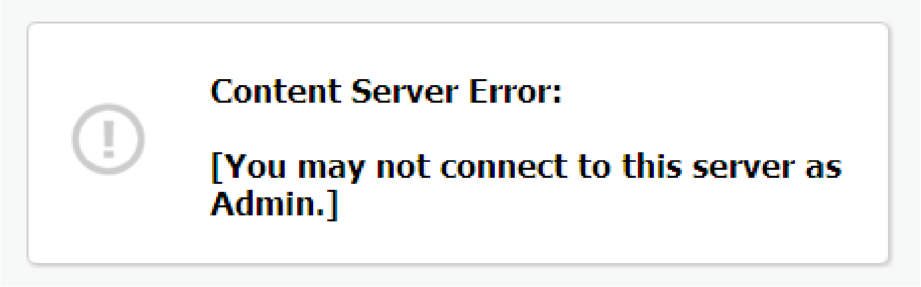
127.0.0.1

The Content Server must be stopped and restarted for these changes to take effect.

Figure 2

It is important to note that some of the functionality that can be accessed through the `admin.index` pages can also be accessed directly through unique URLs. For example, the `Content Server Templates Volume` can be accessed from the main administration page. In this case, the `Limit Admin Account Login` option will only prevent the main administration account (`Admin`) from reaching the Content Server Templates Volume from any IP address other than what is specified. This setting will not prevent access by other accounts that have permissions on the Content Server Templates Volume.

Users who attempt to access the Content Server Administration pages from computers with IP addresses other than those specified will receive the following error message.



Content Server Error:

[You may not connect to this server as Admin.]

Figure 3

Use of this setting does not affect business administrators that perform tasks such as permissions changes. These tasks can be performed on any machine with any IP address.

NOTE: If you have installed OpenText™ Directory Services, the settings you make on this page also prevent the otadmin@otds.admin user from logging on from an unapproved IP address.

DEFAULT SETTING: Field is left blank, allowing access to the `admin.index` page from any IP address.

Configuring Security Parameters

Content Server Administration → Server Configuration → Configure Security Parameters

HTTP-only Cookies

XSSCSRF

This setting controls whether or not authentication cookies (named `LLCookie`) have the HTTP-only attribute. This provides protection from many attacks by preventing many types of client-side scripts from accessing the data in the cookie. This attribute is supported in recent releases of some browsers. For more information about the HTTP-only property, please refer to *Mitigating Cross-site Scripting With HTTP-only Cookies* available on the Microsoft website at http://msdn.microsoft.com/en-us/library/ms533046.aspx.

Administrators should be aware that this feature is not supported by all versions of all browsers. For assistance with determining if a particular browser supports the `HTTP-Only Cookies` feature, please contact support@opentext.com.

NOTE: Enabling HTTP-Only Cookies disables Cluster Management.

DEFAULT SETTING: `Disabled`, therefore authentication cookies will lack the HTTP-Only property.

Cookie Encryption Key

XSSCSRFAUTHENT

Content Server encrypts the data in authentication cookies provided to the user's browser using the AES 256-bit encryption cipher. The cookie is decrypted when it is received by Content Server—part of the normal routine of the application is to authenticate a user.

Every Content Server deployment contains an identical cookie encryption mechanism. And each deployment uses the default encryption key by default. Consequently, an authentication cookie data from one Content Server could be decrypted by another Content Server deployment if both retained the default encryption key. While other security measures may prevent exploiting this issue, administrators can configure Content Server to mitigate this vulnerability.

To prevent decryption of authentication cookie data through other deployments, each Content Server deployment can utilize a unique cookie encryption key. This will make the encrypted data unique to the deployment, and without this unique key, other Content Server deployments cannot decrypt the `LLCookie`.

A value entered in the `Cookie Encryption Key` is used in conjunction with the AES 256-bit encryption for that particular deployment.

If the field is left empty, Content Server uses the name of the installation directory as the encryption key. Administrators should be aware that the Content Server installation routine provides a default installation directory (`C:\OPENTEXT` on Microsoft Windows machines). If Content Server is installed on the default installation directory and the `Cookie Encryption Key` is left blank, the encryption key could be determined easily by an attacker.

NOTE: The `Cookie Encryption Key` must be the same across load-balanced Content Servers.

DEFAULT SETTING: The field is empty; the installation directory name is used as the encryption key.

Data Encryption Key

XSSCSRF

The password used by Content Server to access the database is stored as an encrypted value in the `opentext.ini` file. The information is encrypted using the AES-256 bit encryption cipher.

Every Content Server deployment contains an identical database password encryption mechanism. And each deployment uses the default data encryption key by default. Consequently, a database password from one Content Server could be decrypted by another Content Server deployment if both retained the default data encryption key. While other security measures may prevent exploiting this issue, administrators can configure Content Server to mitigate this vulnerability.

To prevent the decryption of the database password by other deployments, each Content Server deployment can utilize a unique data encryption key. This will make the encrypted database password unique to each deployment and without this unique data encryption key, other Content Server deployments cannot decrypt the encrypted password.

A value entered in the `Data Encryption Key` will be used in conjunction with the AES encryption for that particular deployment.

If the field is left empty, Content Server uses the name of the installation directory as an encryption key. Administrators should be aware that the Content Server installation routine provides a default installation directory (`C:\OPENTEXT` on MS Windows machines). If Content Server is installed on the default installation directory and the `Data Encryption Key` is left blank, the encryption key could be easily guessed by an attacker.

DEFAULT SETTING: The field is empty; the installation directory name is used as the encryption key.

Cookie Authentication Information

Client IP Address

XSSCSRFAUTHENTASR

The `Client IP Address` data can be contained in the encrypted authentication cookie that is provided to the browser by the server. When the user makes a request to Content Server, the authentication cookie is transmitted back to the server. The IP address that is the source of the communication and the IP address stored in the cookie are compared. If there is a difference, the request is denied.

This security feature prevents stolen cookies from being used on computers that have different IP addresses than the source of the cookie.

Content Server can be set to compare the IP address of the source of the communication and the IP address in the cookie with varying degrees of definition. Some Content Server deployments will involve client computers that have IP addresses that may change during a normal period of interaction with Content Server. Administrators should choose the correct option based on the nature of the IP address changes in their environment and their security policy. Best practices suggest matching IP addresses against the largest number of octets without causing any interruption to users.

The following table provides a list of options when Content Server is deployed to support an IPv6 network:

ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff/128 (Compare Entire IP Address)	Compares the entire IP address
ffff:ffff:ffff:ffff:ffff:ffff:ffff::/112	Compares the first seven (7) groups of the IP addresses
ffff:ffff:ffff:ffff:ffff:ffff::/96	Compares the first six (6) groups of the IP addresses
ffff:ffff:ffff:ffff:ffff::/80	Compares the first five (5) groups of the IP addresses
ffff:ffff:ffff:ffff::/64	Compares the first four (4) groups of the IP addresses
ffff:ffff:ffff::/48	Compares the first three (3) groups of the IP addresses
ffff:ffff::/32	Compares the first two (2) groups of the IP addresses
ffff::/16	Compares the first octet of the IP addresses
Do not use IP Address for authentication	Disables this feature

When Content Server is deployed to support an IPv4 network, the options are:

255.255.255.255 **(Compare Entire IP Address)**	Compares the entire IP address
255.255.255.0	Compares the first three (3) octets of the IP addresses
255.255.0.0	Compares the first two (2) octets of the IP addresses
255.0.0.0	Compares the first octet of the IP addresses
Do not use IP Address for Authentication	Disables this feature.

If selected, **Enable X-Forwarded-For for Client IP** mapping tells Content Server to read the client IP address from the `X-Forwarded-For HTTP` header. Otherwise, Content Server reads the IP address from the request. **Trusted Proxy Server List** tells Content Server which `X-Forwarded-For proxy IPs` to trust.

DEFAULT SETTING: 255.255.255.255 (Compare Entire IP Address) or **ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff/128 (Compare Entire IP Address)** (depending upon whether the installation was made on an IPv4 or IPv6 network); Content Server compares the entire IP address within the cookie and of the source of the request.

Owner ID

XSSCSRFAUTHENT

Use of the `Owner ID` option enhances the authentication process between the user's browser and the server.

This option will configure Content Server to include the `Owner ID` in the encrypted payload of the authentication cookie. The `Owner ID` is the unique number assigned by Content Server to the user account that was used to create the particular user.

For example:

- "Bob" creates the user account for "Alice".
- The `Owner ID` associated with "Alice" is the unique id assigned by Content Server for "Bob".

The `Owner ID` is not the `username` that is used during logon. It is the unique number assigned to a user by Content Server. If the `Owner ID` is acquired by an attacker, it would not assist them in gaining unauthorized access to Content Server.

When the user attempts to perform an action on Content Server that requires user permissions, the browser provides the authentication cookie to the server. As part of the user verification process, the server checks the `Owner ID` from the cookie to the `Owner ID` information on the server for that particular user. If the comparison fails, the user's request will not be acted upon.

DEFAULT SETTING: The `Owner ID` checkbox is not selected and the `Owner ID` is not included in the authentication cookie.

Password Expiration Date – 10.5 non-OTDS systems ONLY

XSSCSRFAUTHENT

Use of the `Password Expiration Date` option enhances the authentication process between the user’s browser and the server.

Selecting the check box for this option places the user’s `Password Expiration Date` in the authentication cookie. This information cannot be used by an attacker to gain unauthorized access to Content Server.

When the user attempts to perform an action on Content Server that requires user permissions, the browser provides the authentication cookie to the server. As part of the user verification process, the server compares the `Password Expiration Date` from the cookie against the password expiration date on the server for that particular user. If the comparison fails, the user’s request will not be acted upon.

DEFAULT SETTING: Password Expiration Date is not enabled and the `Password Expiration Date` is not included in the authentication cookie.

One-way Encrypted Password – 10.5 non-OTDS systems ONLY

XSSCSRFAUTHENT

Use of the `One-way Encrypted Password` option enhances the authentication process between the user’s browser and the server.

Enabling this option places information derived from the user’s password in the cookie. The information cannot be decrypted back to the original password.

When the user attempts to perform an action on Content Server that requires user permissions, the browser provides the authentication cookie to the server. As part of the user verification process, the server checks the `One-way Encrypted Password` from the cookie against a one-way encrypted password stored by the server. If the comparison fails, the user’s request will not be acted upon.

DEFAULT SETTING: One-way Encrypted Password is not enabled and the `One-way Encrypted Password` is not included in the authentication cookie.

Expiration

XSSCSRFAUTHENT

This feature controls how long an authentication cookie remains valid before the user has to re-authenticate by logging onto Content Server again. Administrators should analyze the security policy of their organization to decide on the appropriate setting.

There are three options:

1. **Never Expire**

   When this option is enabled, a user will not have to log onto Content Server again as long as the authentication cookie exists in their browser’s cookie cache. If the browser eliminates the cookie—due to user interaction or browser settings—or the cookie is manually removed, the user will have to log onto Content Server. This is the least stringent of the three expiration setting options.

   There are situations however where **Never Expire** would be the desired setting. If the web server is configured to require authentication (such as with NTLM), there is no reason to expire the LLCookie. The user will transparently be logged in again when the cookie expires and this just represents overhead.

2. **Expire ___ minutes after last request**

Administrators can specify the amount of time in minutes that will pass after a user's last request for information from Content Server before the user is required to log on again. The security afforded by this option depends upon the amount of time specified by the administrator for this option. Setting this option for a shorter amount of time for a Content Server deployment whose users interact with Content Server on an infrequent basis may cause users to become frustrated as they are asked to log on frequently. However, in an environment where users are interacting with Content Server frequently during a given time period, setting this option for a shorter amount of time will not require users to log on too frequently.

3. Expire ___ minutes after last log-in

Administrators can specify the number of minutes that will pass after a user logs on before the user is required to log on again. This can be the most stringent user authentication setting if the number of minutes is set appropriately. If the number of minutes is set too low, users will have to log on too frequently.

DEFAULT SETTING: Expire __ minutes after last request option is enabled and number of minutes is set to 30.

Log-in Policies

Disable log-in after ___ failed log-in attempts

AUTHENT

Administrators should set this option according to their organization's security policy. It can be used to prevent attackers from attempting to guess a user's password through trial and error. Setting the number too low will cause users that fail to enter their password correctly to frequently seek help from administrators to re-enable their accounts. Administrators can enable the **Send e-mail to the Administrator when log-in is disabled** option. Once enabled, this option will set Content Server to send an email message to the Administrator when a user's account is disabled because of the number of failed log-in attempts. Administrators should analyze the Content Server logs for accounts that are frequently disabled as it may indicate attempts to gain unauthorized access.

To change the email account to which messages are sent, administrators need to change the value in the opentext.ini file in for the entry AdminMailAddress= in the [general] section.

Attempts to guess a user name that does not exist in the system are not affected by this setting.

DEFAULT SETTING Disable log-in after ___ failed log-in attempts is enabled, the number of failed logon attempts is set to 5 and **Send e-mail to the Administrator**

when log-in is disabled is enabled. Content Server will disable accounts automatically when there have been 5 failed logon attempts for that account.

Allow log-in via HTTP GET request

The **Allow log-in via HTTP GET request** setting specifies the default logon behavior. When this option is enabled, users are allowed to sign in to Content Server using an HTTP `Get` request, which stores their sign-in credentials in a bookmark. When this option is disabled, users are required to sign in again when that session's cookies expire.

DEFAULT SETTING: This option is disabled by default.

Require Secure Request Token

The **Require secure request token** setting, if enabled, helps to prevent cross-site request forgery: an attack whereby a user unknowingly initiates an action that takes place in software to which the user has already logged on. The secure request token is a value that is shared from the server to the browser when the user performs certain actions. This value must accompany requests for other actions. If the value is not present, the requested action is invalid.

DEFAULT SETTING: This option is disabled by default.

Disable simultaneous sessions from multiple machines, except for hosts: ______

AUTHENT

This feature prevents simultaneous logons from machines with different IP addresses. It is an effective measure against unauthorized access attacks. Administrators should enable this option as dictated by their security policy.

In some instances, multiple machine logons may need to be enabled on selected computers. The IP addresses of the machines can be entered in the space provided.

DEFAULT SETTING: Disable simultaneous sessions from multiple machines, except for hosts: ______ is not enabled, so simultaneous sessions from all hosts are allowed.

Log-in Page Configuration

Disable Browser Autocompletions – 10.5 non-OTDS system ONLY

AUTHENT

Modern browsers can automatically complete data being entered in a form field if the user has previously entered data into the same field. This subverts the authentication process as the user of a browser can simply start typing a user name or password into the logon screen and the browser will "autocomplete" the entry of the data. This could allow an attacker to gain unauthorized access if they were to be able to access another user's workstation's browser that had been used to access Content Server. Administrators should consider using this feature to enhance user authentication.

It is important to note that unless an entry is made in the **Number of Days Password Persists** field, the **Disable Browser Autocompletions** feature will not operate. Administrators must set a number of days a password will persist.

Administrators should be aware that not all versions of all browsers support this feature. For assistance in diagnosing if a particular browser does support the **Disable Browser Autocompletions** feature, please contact support@opentext.com.

DEFAULT SETTING: **Disable Browser Autocompletions** is enabled, instructing browsers to not allow autocomplete on the logon page.

Number of Days Password Persists

AUTHENT

Administrators can enable a **Remember Password** check box on the logon page when they enter any number greater than zero (0) in this field. Users who enable this setting when logging on will have a permanent authentication cookie saved on their computers for the specified number of days. This value does not override the cookie Expiration value set in the Cookie Authentication Information section above.

DEFAULT SETTING: The field is empty; the password will not persist in the browser for the autocomplete feature.

Frame Embedding

CSRF

Protects request handlers from clickjacking attacks by preventing embedding in external frames.

NOTE: Specific settings are required for this feature in Microsoft SharePoint, Extended ECM for SAP, Process Component Library

DEFAULT SETTING: The option is enabled; request handlers are prevented from being embedded in external frames.

Request Argument Filtering

XSSCSRFSQL

All client requests to Content Server are compared with the values in the **Filter String** field when request-argument filtering is enabled. If values in the request match those in the **Filter String**, the request is rejected.

The filter list is delimited by a separator that is specified in the **Separator Character** field. For example, if the **Separator Character** is set to be a comma (,) different filter strings would be entered as:

```
Sting1,String2,String3
```

The choice of separator should be made according to the desired strings to be filtered. For example if a filter string of “`apples and pears`” is entered, using a separator of “`and`” would break the string inappropriately.

It is important to note that Content Server functions can be affected by Request Argument Filtering. This can be used to prevent access of administration functions (by entering `admin.` into the Request Argument Filtering field will stop all access to the administrator pages—such as the `admin.index` page). It can also break functionality that supports users if words associated with Content Server functionality are entered as Request Arguments.

DEFAULT SETTING: The field is empty; Content Server will not filter requests.

Container Size Display

ASR

Content Server containers can store many unique items. The number of items is displayed in the **Size** column when browsing Content Server. In a similar manner to the number of replies to a search query, this is an absolute value unaffected by permission settings and thus may “leak” information that is otherwise unavailable to the user. This information can be suppressed so that the number of items in a container is not indicated. This may be desirable depending on an organization’s security policy.

DEFAULT SETTING: The setting is not enabled; this allows the number of items in a container to be displayed.

Secure Request Token Expiration

CSRF

OpenText has identified key security-centric functions that should receive additional protection from Cross-site Request Forgery attacks. The list of identified functions can be found in Appendix A – Functions with Secure Request Token Mechanism.

The Secure Request Token mechanism is best explained using the following example:

A user wishes to change the permissions on a document in Content Server. When they invoke the **Permissions** page, Content Server provides an encrypted token to the user as part of the delivery of the **Permissions** page. The secure request token contains:

- A unique identifier of the user that invoked the Permission page request;
- A time-based expiration value.

The user navigates to the **Permissions** page and sets the new permissions. When they click **Apply**, the browser submits the requested permission changes and the secure request token to Content Server.

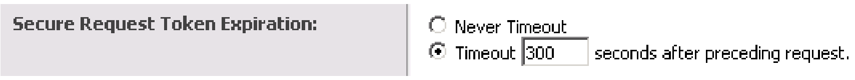
Initially, Content Server attempts to decrypt the secure request token. If the decryption fails, the request does not proceed. This helps to prevent against attacks through modification of the encrypted secure request token.

If the secure request token is successfully decrypted, Content Server inspects the values as follows:

- The unique identifier of the user that invoked the **Permissions** page request. (This value must identify the same user as is referenced by the encrypted authentication cookie that accompanied the request. This helps prevent attacks against the secure request token through re-use under different user accounts.)

- The time expiration. The secure request token is only valid for a short amount of time. This helps prevent re-use by attackers. If the token comes back to Content Server after it expires (or from another user) the request will fail.

Only the expiration time limit can be set for this feature. Unique user identifier and information about the preceding request are provided by Content Server.



Secure Request Token Expiration: ○ Never Timeout ● Timeout 300 seconds after preceding request.

DEFAULT SETTING: The **Timeout ___ second after preceding request** option is set to `300` seconds. Administrators may want to adjust this time based on the deployment's capacities. Administrators have the option to remove the token expiration completely by enabling **Never Timeout**. It should be noted that removing the token expiration weakens the security afforded by this mechanism.

Content Server Client Hosts

AUTHENT

This configuration option allows administrators to restrict the IP addresses of those servers that work in conjunction with the Content Server—such as web servers, file servers, and Admin servers.

If elements of the Content Server are located on the same server as the Content Server itself, the loop-back address—for IPv4 addressing, this is `127.0.0.1`—and the host's routable IP address should be entered. By leaving the field empty, any server can communicate with the Content Server service.

Content Server Client Hosts:

DEFAULT SETTING: The field is blank; any server may communicate with the Content Server.

Trusted Referring Websites

CSRFAUTHENT

Users can interact with Content Server through a web browser. Through the browser, a user could view a website / page created by an attacker. This website / page could contain active scripts that could attack Content Server.

To mitigate these attacks, Content Server examines the `referrer` or `Http referrer`. This is the URL of the last page that the user has visited through the browser before sending the request. Use of the `referrer` is standard functionality for all modern browsers and web services.

Content Server examines the `referrer` whenever a user interacts with Content Server. If the request is coming from a browser that was visiting a website other than those in the **Trusted Referring Websites** list, the request is denied and the user is prompted to log on.

Administrators should include any websites that will direct users directly to documents in the list of **Trusted Referring Websites**. This will allow users of browsers that currently have valid authentication cookies to access the documents without having to log on again.

It is recommended that referring websites be added only when a business requirement exists, and the content on those sites is **trusted and secure**. If a referring site has a Cross-site Scripting (XSS) vulnerability, it may be possible to attack Content Server using that site as a proxy.

The complete URL of all trusted referring websites should be entered in the field provided. Each website address should be entered on a separate line in the Trusted Referring Websites field.

Trusted Referring Websites:

DEFAULT SETTING: The field is blank; only the originating Enterprise Server site is a trusted referrer.

Document Functions

Open

EXTERNAL

Content Server can use file type associations to automatically open documents in the correct desktop application. To allow this functionality, select the `Enabled` option. Some organizations may have security policies that do not support documents being automatically opened based on file type association. By selecting the `Disabled` option, users are forced to download the document and then open it manually.

DEFAULT SETTING: The `Disabled` radio button is selected; Content Server will not show the `Open` option to users.

View as Web Page

XSS CSRF

Content Server can render certain types of documents as webpages. Administrators should be aware that rendering certain documents as webpages may introduce some vulnerabilities. Some documents may include active script or other items that a browser may render or act upon, potentially causing security vulnerabilities. Opening the document in its native application or in a viewer application may help to avoid these vulnerabilities.

Administrators should evaluate the usefulness of the **View as Web Page** option for Content Server users versus the risk for vulnerabilities to be introduced when using a web browser to render documents.

To enable the **View as Web Page** functionality for users, select the **Enabled** option. By selecting the **Disabled** option, the **View** option will not be shown. Users can **Open** or **Download** the documents.

DEFAULT SETTING: The **Enabled** radio button is selected; Content Server will show the **View as Web Page** option to users.

Trusted Cross Domains

XSS CSRF

The Trusted Cross Domain functionality allows administrators to inform Content Server that JavaScript from specified servers is approved and can be trusted to interact with JavaScript from Content Server.

OpenText provides a number of products that can leverage and enhance Content Server functionality. These products are best run on separate servers from those running Content Server. Data requests and responses flow amongst the servers in this kind of deployment. Users view webpages that are created by a multitude of services running on multiple servers.

In some deployments, the user may view a webpage that consists of sections that come from Content Server and other servers. Each server will have a unique name (per networking requirements). In this example, the Content Server is called `CS_Server` and the server providing another service is called `OTHER_Server`.

Most browser security policies prevent JavaScript—running in the browser—provided by one server from accessing JavaScript functionality provided by another server. This policy is referred to as “the same origin” policy and its function is to prevent JavaScript in one server from being attacked by JavaScript in another server as it runs in the browser.

When Content Server and another server are working together, there may be a need for the JavaScript from the two servers to work together. By entering the value of `OTHER_Server` in the **Trusted Cross Domains** box, administrators can allow JavaScript from Content Server and the `OTHER_Server` to work together.

DEFAULT SETTING: The **Trusted Cross Domains** box is empty; Content Server will not interfere with the same origin policy restrictions as enforced by the user’s browser. JavaScript provided by a server other than Content Server will not be allowed to access methods in JavaScript provided by Content Server. The same origin policy enforcement is a function of the user’s browser. There are differences in the enforcement of this policy amongst browsers and different versions of browsers.

Document Undelete – Content Server 10.5 Only

Content Server Administration → Document Undelete Administration

Undelete is available on Content Server 10.5 systems that do not have the Recycle Bin module installed.

Configure Autopurge

PRIVACY

Content Server stores deleted items in the Undelete Volume for a specified period of time before deleting them permanently. The number of days that deleted documents are retained before being removed from the Undelete Volume should be set in accordance with an organization's security policy.

The number of days is used to calculate the number of twenty-four hour periods that have passed since the document was deleted by the user. When the number `7` is entered into the `Days Old` field, documents are set to be purged from the Undelete Volume after 168 hours (7 x 24 hours). The purge process runs automatically every 5 minutes.

This setting only applies to Documents. Other Content Server items, including Compound Documents, are not affected by this setting.

DEFAULT SETTING: The **Days Old** field is set to a value of `7`; items are purged after 168 hours (7 x 24 hours)

Purge Deleted Documents

EXTERNAL

Administrators can perform purges of the Undelete Volume on command using this feature. To delete all documents in the Undelete Volume, set **Days Old** to `0` (zero). To retain documents that are less than `7` days old, enter `7` (seven) in the **Days Old** field.

The number of days is used to calculate the number of twenty-four hour periods that have passed since the document was deleted by the user. When the number `7` is entered into the **Days Old** field, documents that were deleted less than 168 hours (7 x 24 hours) before the time that the administrator invokes the `Purge` function are retained and all others are deleted.

This setting only applies to Documents. Other Content Server items, including Compound Documents, are not affected by this setting.

DEFAULT SETTING: The **Days Old** field is set to a value of `7`; deleted items that are greater than 168 hours (7 x 24 hours) are purged.

Immediate Deletion of Documents

EXTERNAL

Some organizations require that documents be deleted without the possibility of restoration or retrieval. The Content Server Document Undelete module can be uninstalled from Content Server through the **Content Server Administration → Module Administration → Uninstall Modules** interface.

DEFAULT SETTING: The module is installed by default, allowing for the recovery of deleted documents.

Recycle Bin Settings – Content Server 16.0 Only

The Recycle Bin Module was an optional module with Content Server 10.5 and earlier. Recycle Bin is no longer an optional module for Content Server 16, the Recycle bin functionality has been integrated into Content Server 16.0. By default, Content Server 16 is installed with the Recycle Bin enabled, so that an item that has been deleted can be restored to Content Server.

When a user deletes an item, Content Server places the item in the Recycle Bin. The Recycle Bin allows any user that could delete the item from its original location to restore the item or purge it from the Recycle Bin. Items that are purged from the Recycle Bin are permanently deleted.

Not every item type can be restored after it is deleted. Content Server is capable of restoring a wide variety of deleted item types, but certain non-restorable item types are not placed in the Recycle Bin when they are deleted

Supported Types

Restorable

Click **Edit/Review Restorable Node Types** to view a listing of items that Content Server can restore. Item types that appear in the **Mandatory** section are always restorable. You cannot configure them. Item types that appear in the **Optional** section are configurable. If you enable one of the item types in this section, deleted items of that type are placed in the Recycle Bin. If you disable one of them, items of that type are purged immediately upon deletion and cannot be restored.

EXTERNAL

Not Restorable

Click **Review Non-Restorable Node Types** to view a listing of item types that Content Server cannot restore. These item types can never be made restorable.

EXTERNAL

Settings

Enable

EXTERNAL

You can enable or disable the Recycle Bin in your Content Server deployment. If you disable the Recycle Bin, deleted items cannot be restored and are scheduled for purge immediately upon deletion.

Select **Enable Recycle Bin** to enable the Recycle Bin or **Disable Recycle Bin** to disable the Recycle Bin.

DEFAULT SETTING: The default setting is **Enable Recycle Bin**: Allow restore for supported object types

Purging

EXTERNAL

To retain deleted items in the Recycle Bin until a user purges them, enable **Keep deleted items until manually purged**. To configure Content Server to automatically purge deleted items in the Recycle Bin after a period of time, enable **Purge items automatically** and specify a number of days in the box before **Days to retain before purging**.

If you want the Recycle Bin to display the date that Content Server is scheduled to purge an item from the Recycle Bin, enable **Display purge date column in Recycle Bin**. If this setting is enabled, the Recycle Bin displays a **Purge Date** column in addition to the columns that appear by default (**Type**, **Name**, **Size**, **Deleted By**, **Deleted Date**, and **Location**).

DEFAULT SETTING: The default setting is **Purge items automatically** with a default of `60` **days to retain before purging**. **Display purge data column in Recycle Bin** is disabled by default.

User Options

User Access

EXTERNAL

To allow users access to the Recycle Bin, enable **Ordinary users can see Recycle Bin**. If this setting is not enabled, users do not have a **Recycle Bin** option in their **Tools** global menu. If the setting is enabled, the **Recycle Bin** option does appear in their **Tools** global menu, and they can use it to access the Recycle Bin and restore deleted items. If you wish to also allow users to purge items from the Recycle Bin, enable **Users can Purge items**.

DEFAULT SETTING: The default setting is that **Ordinary users can see the Recycle Bin** is enabled and **Users can Purge items** is disabled.

User View Options

EXTERNAL

The options in the **User View Options** section enable the appearance of various filters that can be used to regulate the appearance of the Recycle Bin. Disabling a filter prevents Content Server users from seeing and using it in the Recycle Bin. It has no effect on Recycle Bin Managers or users with the `System Administration rights` privilege.

Important:
Enable at least one filter if you want Content Server users to have access to the Recycle Bin. Disabling every filter has the same effect as disabling **Ordinary users can see Recycle Bin**: it removes the **Recycle Bin** option from their **Tools** global menu.

DEFAULT SETTING: The default settings are that the following User View options are enabled: **I Deleted Today**, **I Deleted**, **Anyone Deleted Today**, **Anyone Deleted**

Content Server “About” Page Requiring Authenticated Access

Content Server Administration → Server Configuration → Configure Server Parameters → Default User Start Page

Content Server’s **About** page is available without authentication by default through the URL `http://server_name/OTCS/cs.exe?func=ll.index`

This page discloses the version of Content Server and other associated software used by Content Server that may be considered confidential information.

"About Content Server" Requires Login

EXTERNALPRIVACY

If an organization’s security policy dictates that this information is to be kept confidential, administrators can control this by enabling **"About Content Server" Requires Login**.

DEFAULT SETTING: "About Content Server" Requires Login is not enabled; all users can access the **About** page.

Secure Cookie Settings

Setting Secure Cookies in Content Server using the opentext.ini Setting

Secure Cookies

This setting controls the setting of the secure flag for the user's logon cookie. If Content Server is running on an HTTPS server, SSL, the secure flag will be set for the user's logon cookie.

Edit the `opentext.ini` file in the `config` folder in <OTHOME> and, in the `[options]` section, add the `wantSecureCookies` parameter

Syntax:

```
wantSecureCookies=TRUE
```

Values:

`TRUE` or `FALSE`. The default value is `TRUE`.

Setting Secure Cookies in **OTDS**

For systems using OTDS this setting must also be set in OTDS. To do this set `otds.as.wantSecureCookies` from the OTDS admin page.

User Password Settings – Content Server 10.5 non-OTDS Systems

Content Server Administration → Users and Groups Administration → Configure Password Settings

Administrators should evaluate the requirements of their security policy and configure the password settings accordingly. If alternative account management services are used—such as LDAP integration—these settings are ignored.

Minimum Number of Characters

AUTHENTPRIVACY

This sets the minimum number of characters that can be used in a user password.

DEFAULT SETTING: The value is set to `6` (six).

Passwords Must Contain a Digit

AUTHENTPRIVACY

When the **Enable** checkbox is selected, user passwords are rejected if they do not contain a numeric value (a digit).

DEFAULT SETTING: The **Enable** checkbox is selected; passwords require a digit.

Password Cannot Begin With a Digit

AUTHENTPRIVACY

When the **Enable** checkbox is selected, user passwords are rejected if they begin with a digit.

DEFAULT SETTING: The **Enable** checkbox is not selected; passwords may begin with a digit.

Password Cannot End With a Digit

AUTHENTPRIVACY

When the **`Enable`** checkbox is selected, user passwords are rejected if they end with a digit.

DEFAULT SETTING: The **`Enable`** checkbox is not selected; passwords may end with a digit.

Changed Password Must Be Different

AUTHENTPRIVACY

When the **Enable** checkbox is selected, a user must change their password to a value other than the previously used password.

DEFAULT SETTING: The **Enable** checkbox is selected; users cannot re-use their previous password when they are prompted to change their password.

Change Password at First Login

AUTHENTPRIVACY

When the **Enable** checkbox is selected, a user must change their password when they first log on to Content Server. An organization's security policy may dictate that this function is enabled to prevent users from using passwords provided by system administrators—which are often default or simple phrases.

DEFAULT SETTING: The **Enable** checkbox is selected; users are prompted to change their passwords when they log on for the first time.

Password Expiration

AUTHENTPRIVACY

When **on** is enabled, users will be notified that their password will expire. The **Days Before Expiration** field is used to determine how many days (24-hour periods) ahead of the password expiration that users are notified that their password will expire. When the **Off** radio button is selected, users are not notified of the upcoming password expiration.

DEFAULT SETTING: On is enabled and **Days Before Expiration** is set to `30`; users are notified that their password will expire.

Days to Prevent Password Re-use

AUTHENTPRIVACY

Users can be prevented from re-using the same password for a set number of days. The options are `0`, `5`, `10`, `15`, `30`, `45` and `60` (days). When a value other than `0` is selected, users cannot reset their password to a password they have used in the past for the number of days specified.

This is different than the **Changed Password Must Be Different** option. An example would be that a user would change their password from `apple` to `orange` to meet the **Changed Password Must Be Different** requirement. However, they could immediately change their password back from `orange` to `apple`. This setting determines how many days need to pass before the password can be successfully changed back to `apple` for this example.

DEFAULT SETTING: The value is set to sixty (`60`); users cannot re-use passwords previously used in the past 60 days.

Days Required Between Password Changes

AUTHENTPRIVACY

Users can be prevented from changing their password for a set number of days. The options are `0`, `1`, `5`, `10`, `15`, and `30` (days). This setting can help prevent users from needlessly changing their passwords frequently, causing them to forget their current password. This may lead to unnecessary support calls, users choosing weaker passwords, and writing passwords down in order to remember them.

DEFAULT SETTING: The value is set to zero (`0`); users can change their password again immediately after changing their password.

User Password Settings – Content Server 16.0 and 10.5 OTDS

In Content Server 16.0 and later, OpenText Directory Services is integrated into the product. Password settings are done through OTDS.

Password Quality

Minimum number of characters

AUTHENTPRIVACY

This sets the minimum number of characters that can be used in a user password.

DEFAULT SETTING: The minimum number of characters is set to six**.**

Minimum number of digits

AUTHENTPRIVACY

This sets the minimum number of digits that can be used in a user password.

DEFAULT SETTING: The minimum number of digits is set to one.

Minimum number of symbols

AUTHENTPRIVACY

This sets the minimum number of symbols that can be used in a user password.

DEFAULT SETTING: The minimum number of symbols is set to zero.

Minimum number of uppercase characters

AUTHENTPRIVACY

This sets the minimum number of uppercase characters that can be used in a user password.

DEFAULT SETTING: The minimum number of uppercase characters is set to zero.

Minimum number of lowercase characters

AUTHENTPRIVACY

This sets the minimum number of lowercase characters that can be used in a user password.

DEFAULT SETTING: The minimum number of lowercase characters is set to zero.

Minimum number of changes to previous password

AUTHENTPRIVACY

This sets the minimum number of changes that you require to make to their previous password.

DEFAULT SETTING: The minimum number of changes to previous password is set to zero.

Number of unique passwords before an old password can be re-used

AUTHENTPRIVACY

This sets the number of passwords that must be unique before a previously used password can be used again.

DEFAULT SETTING: The number of unique passwords before an old password can be re-used is set to three.

Security Options

Password can be changed in (days)

AUTHENTPRIVACY

This sets the minimum number of days before a new password can be changed.

DEFAULT SETTING: Password can be changed in (days) is set to one.

Password expires in (days)

AUTHENTPRIVACY

This sets the number of days before the password expires and must be changed.

DEFAULT SETTING: Password expires in (days) is set to thirty.

Lockout failure count

AUTHENTPRIVACY

This sets the maximum number of invalid password attempts before the user is locked out.

DEFAULT SETTING: Lockout failure count is set to three.

Lockout duration (minutes)

AUTHENTPRIVACY

This sets the number in minutes that a user will be locked out from their account if they exceed the maximum number of invalid password attempts.

DEFAULT SETTING: Lockout duration (minutes) is set to 15.

User name Display Control

EXTERNALPRIVACY

Content Server Administration → Users and Groups Administration → Configure User Name Display

The security policy of an organization may dictate what information can be displayed on pages delivered by Content Server. There are several options available. These include:

```
Log-in ID
```

```
FirstName LastName
```

```
FirstName MiddleInitial LastName
```

```
LastName, FirstName
```

```
LastName, FirstName
MiddleInitial
```

```
LastName FirstName
```

DEFAULT SETTING: This option is set to **Log-in ID**; only the user's log-in id is displayed.

Append (Log-in ID)

EXTERNALPRIVACY

This will add the log-in id of the user to the value as selected in the **User Name Display** menu.

DEFAULT SETTING: The checkbox is not selected; Content Server will not add the log-in id to the user name for display. The checkbox is grayed out by default as the default **Display Name Format** is **Log-in ID**.

Configure Access Control

Content Server Administration → System Administration → Configure Access Control

Content Server allows administrators to configure the degree of control users have over the permissions on objects stored within the Content Server repository.

Default Access

Restrict "Grant Access' to Groups only.

EXTERNAL

By enabling this option, administrators prevent users from assigning permissions based on individual user accounts. Users can assign permissions for Groups only. This is most effective in environments where Role Based Access Control models are observed.

Restrict restoring "Owner Access" to System Administrators

EXTERNAL

By enabling this option, administrators can prevent users from restoring access for the owner of a document if the administrators have removed the access privilege. If a user can restore owner access, the owner can effectively reverse any permission restriction set by administrators.

Restrict restoring "Owner Group Access" to System Administrators

EXTERNAL

By enabling this option, administrators can prevent users from restoring access for the owner group of a document if the administrators have removed the access privilege. If a user can restore owner group access, the owner group can effectively reverse any permission restriction set by administrators.

Restrict restoring "Public Access" to System Administrators.

EXTERNAL

By enabling this option, administrators prevent all users from assigning the Public Access permission to any item that has had the Public Access permission removed. This option is available as the Public Access group is by default a group that includes all users.

DEFAULT SETTING: None of the checkboxes are selected; no restrictions are in place on the granting of access (access can be granted to groups or individual users), the restoration of Owner Access, Owner Group Access or Public Access privileges.

Moving Items across Workspaces

Always inherit the permissions from target destination

EXTERNALPRIVACY

When a document is moved from one workspace to another, there is a question as to how the permissions should be set on the document. An example would be a financial report document. Its original workspace set the permissions so that it restricted access to the document to only those people in the financial reporting area. When the document is made public as part of the financial reporting obligations of the corporation, it is moved to the Enterprise Workspace, where the default permission setting makes documents available to a wider membership of the organization.

By selecting this option, the financial report would lose the original permission settings and gain those that are set for the destination workspace (in this example, the document would now be available to a wide array of users). If this option is not selected, the financial report will continue be restricted to the people in the financial reporting area—as was provided by the original workspace.

Administrators should consider their organization’s security policy when deciding which model of permission provisions they will use. It is a best practice to teach users to review the permissions on items when they move them from one workspace to another, regardless of which option is selected.

DEFAULT SETTING: This setting is not enabled; the original permissions of the document are maintained when it is moved and the permissions of the target destination are not applied.

Configuring For Least Privilege

EXTERNALPRIVACY ASR

The principle of least privilege is that only those privileges needed to ensure proper operations are provided to a resource. Administrators need to ensure that Content Server deployments are operating under system accounts that use the least privileges required to run the application. This ensures:

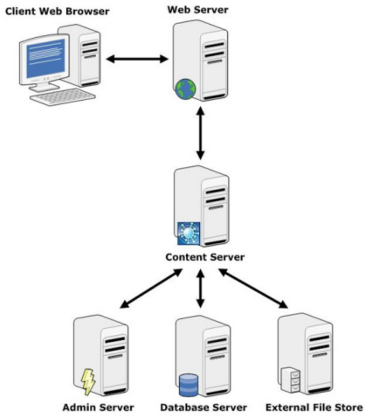
- Improved stability – prevents inadvertent interaction with system resources that are not required by the application
- Improved security - prevents unwanted access to resources outside those required by the application.

Typical Deployment Scenarios

Content Server is an *n*-tier application. This architecture enhances security as it prevents direct client access to stored content. This architecture allows security features in the web server, Content Server system, database server, and Extended File Store along with network firewalls to be used to prevent unauthorized access.

Content Server can be deployed in many different configurations. A typical sample deployment is as follows:

Figure 4



The web server, Admin Server, database server, and file store can be on the same logical or physical server as Content Server or on multiple logical or physical servers.

Service Accounts

The directory where Content Server is installed is referred to as `<OTHOME>`.

There are three services that are part of a Content Server install:

1. Content Server
2. Content Server Admin
3. Content Server Cluster Agent

These services can run under a domain or system user account. This type of account can be assigned limited privileges but requires the following privileges and permissions:

NOTE: Detailed instructions on configuring privileges and permissions listed below are available in Appendix D – Securing Content Server Services.

1. The `Log On as a Service` privilege on the system running Content Server.
2. The `Stop`, `Start`, `Pause`, `QueryConf`, `ChangeConf`, `QueryStat`, and `Interrogate` permissions.
3. `Modify` permissions to the External File Store. This is commonly located on another server or a SAN.
4. The following folder permissions:

<OTHOME>	Read & Execute, List Folder Contents, Read
<OTHOME>\bin	Read, Execute
<OTHOME>\cache	Modify
<OTHOME>\cgi	Read, Execute
<OTHOME>\config and all subdirectories	Modify
<OTHOME>\csapplications (10.5 only)	Modify
<OTHOME>\csapplicationsstaging (10.5 only)	Modify
<OTHOME>\filters and all subdirectories	Read, Execute
<OTHOME>\index and all subdirectories	Modify
<OTHOME>\logs	Modify
<OTHOME>\module	Modify
<OTHOME>\staging	Modify
<OTHOME>\support	Modify
<OTHOME>\temp and all sub directories	Modify
<OTHOME>\tmp (10.5 only)	Modify
<OTHOME>\viewcache[1]	Modify

Internet Information Server Account Requirements

Content Server works with a number of web servers including Internet Information Server (IIS). Deployments using IIS have specific requirements.

By default, the path for Content Server logs is set as .\logs\ in the opentext.ini file (Logpath=.\logs\). If the value for Logpath remains .\logs\, the IUSR account must have read access to the **<OTHOME>** directory to reach the logs directory. Administrators can set a defined path (such as D:\opentext\logs or /logserver/opentext/logs) for the Logpath option. Under that configuration, the IUSR account does not need read access to the **<OTHOME>** directory but does require Modify permissions to the **<OTHOME>\logs** directory.

IIS creates an account called IUSR. The IUSR account requires specific access to folders under the **<OTHOME>** directory:

<OTHOME>\cgi	Read, Execute
<OTHOME>\config	Read, Execute
<OTHOME>\res	Read, Execute
<OTHOME>\support	Read, Execute
<OTHOME>\logs	Modify
<OTHOME>\viewcache	Modify
<OTHOME>\upload	Modify + Advanced > change permissions > edit. Select also delete subfolders and files - everything should be checked except full control, change permissions and take ownership.

IIS creates a user group called IIS_IUSRS. This group also requires specific access to folders under the **<OTHOME>** directory:

<OTHOME>\cgi	Read, Execute
<OTHOME>\config	Read, Execute
<OTHOME>\res	Read, Execute
<OTHOME>\support	Read, Execute
<OTHOME>\logs	Modify
<OTHOME>\upload	Modify + Advanced > change permissions > edit. Select also delete subfolders and files - everything should be checked except full control, change permissions and take ownership.

Notifications Administration

Content Server Administration → Notification Administration

Content Server has a number of notification settings that control how and when notifications are sent to users. Administrators should ensure notification delivery is set correctly to ensure that all events are sent in a timely manner.

Configure Notification

Content Server Administration → Notification Administration → Configure Notification

Administrators should enter the proper settings to allow the Content Server deployment to communicate with the corporate SMTP gateway.

Administrators should set the Default Notification Schedules according to the security policy and operational policy of their organization. It is important that notifications be reviewed in a timely manner to ensure that security-related events are addressed quickly.

Enable Notifications

EXTERNAL

To enable Notifications, select the **Enable** radio button for the **Enable Notification**s option.

DEFAULT SETTING: The **Enable** radio button is not selected; notifications are not sent.

Notification Schedule(s)

EXTERNAL

Administrators should set the **Default Notification Schedules** according to the security policy and operational policy of their organization. It is important that notifications be reviewed in a timely manner to ensure that security-related events are addressed quickly.

DEFAULT SETTING: Default Notification Schedule 1, **Default Notification Schedule 2** and **Default Notification Schedule 3** are all set to send notifications from 9:00 A.M. to 4:00 P.M. on the hour (according to the server's time) from Monday to Friday (according to the server's date).

Configure Scheduled Activities

Content Server Administration → Notification Administration → Configure Scheduled Activities

There are multiple activities that can be scheduled through this interface. This document only addresses those that relate directly to the security of Content Server.

Expire Passwords (Content Server 10.5 Only)

AUTHENT

This function allows administrators to disable accounts that have expired passwords. This is useful for administrators to secure their Content Server deployment against the abuse of accounts with expired passwords.

To use this functionality, first select the **Enabled** radio button. By default, Content Server will disable all accounts with expired passwords every day of the week at midnight. Administrators can change the **Activity Schedule** according to their needs.

DEFAULT SETTING: The **Disable** radio button is selected; no expiration of passwords will occur.

Monitor Password Expiration (Content Server 10.5 Only)

AUTHENT

This feature can help to reduce calls to support from users having password reset issues. By selecting the **Enable** radio button and then entering the numbers of days for the **Send first e-mail ___ day(s) before expiration** and the **Send daily e-mails starting ___ day(s) before expiration** settings, administrators can configure Content Server to remind users that their passwords are going to expire.

An organization's security policy may not support this activity as the message is delivered to the user through email which some organizations consider to be not secure. Administrators should review the contents of a password expiration notification message to ensure that it does not present any unwanted information over a potentially not secured email service.

DEFAULT SETTING: The **Disable** radio button is selected; no monitoring of password expiration will occur.

Failed Log-in Notification

AUTHENT

This feature will generate a report that lists those accounts that have had failed logon attempts. To have these reports generated, select the **Enabled** radio button.

Using the **Activity Schedule** section, administrators can define how often these reports are generated. This schedule should be set in conjunction with the **Activity Schedule** set for **Notification Delivery** which is the process that delivers the reports to the SMTP server.

The **Notify Administrator Threshold** is the key to this report. Administrators can set values for the **Failed log-ins exceed ___within ___ minutes** option boxes. This should be done according to an organization's security policy.

DEFAULT SETTING: The **Disable** radio button is selected; no notification of failed logon attempts will occur.

Logging

Content Server Administration → Search Administration → Configure Debug Settings

Content Server has several logging options that help alert administrators to potential security issues and provide in-life performance statistics. Logs may contain names of documents, users, and other potentially sensitive information. This document addresses only those that relate directly to the security of Content Server.

Administrators should be familiar with the default logging levels for the **Search Administration** services. If logging levels are increased above the default level, the logging processes may create logs that contain information that an organization may consider sensitive. Administrators should be aware of the content of these logs and secure them appropriately.

Content Server Debug Level

EXTERNALPRIVACY

Increasing the number increases the amount of information collected by the logs. For a normal, secure operation this should be set to the default value of zero (`0`).

DEFAULT SETTING: The **Content Server Debug Level** is set to zero (`0`); only errors are noted in the logs.

Log Connections

EXTERNALPRIVACY

This logs the inbound connections to Content Server. Selecting this option will create logs in the `<OTHOME>/Logs` folder. Administrators should secure this directory and the logs that are created through the use of this option.

DEFAULT SETTING: This checkbox is not selected; connection information is not logged.

Log Content Server Timings

EXTERNALPRIVACY

Setting this option configures Content Server to log the timings of the various parts of a Content Server request when the debug level is greater than zero (`0`).

DEFAULT SETTING: This checkbox is selected; Content Server timings will be recorded when the debug level is greater than zero (`0`).

Verbose Logging

EXTERNALPRIVACY

This setting increases the verbosity of any logging to the Content Server connection and timings when the debug level is greater than zero (`0`).

DEFAULT SETTING: This checkbox is selected; Content Server connection and timings will be recorded with a greater level of verbosity when the debug level is greater than zero (`0`).

Summary Timings

EXTERNALPRIVACY

This setting can only be changed by modifying the `opentext.ini` file.

```
 [options]
WantSummaryTimings=TRUE
```

This option creates a comma-delimited file for each running thread with a single-line summary for each transaction of that thread. This file contains enough information to indicate each user’s activity of the system—provided each active server has this option set—and should be considered sensitive. This option was designed to be enabled during normal operation.

DEFAULT SETTING: This option is not enabled by default; it must be explicitly added to the `opentext.ini` file. When enabled, a log with summary of each transaction per thread is created.

Log File

EXTERNALPRIVACY

Logs are created in the `<OTHOME>/Logs/admserv.log` file. If an alternative path and file name are set, administrators should be aware that these logs may contain sensitive information about the Admin server and admin activities. These should be secured appropriately.

DEFAULT SETTING: Logs are created in the `<OTHOME>/Logs/admserv.log` file for the OTAdmin (Admin Server).

Log Level

EXTERNALPRIVACY

For normal operation, this should be set to the default value of one (`1`) which will log only errors. Selecting higher numbers will increase the logging in the admin logs.

DEFAULT SETTING: `Log Level` is set to one (`1`) which will only log errors of the Content Server Admin Server.

Control IP Access to Search Components

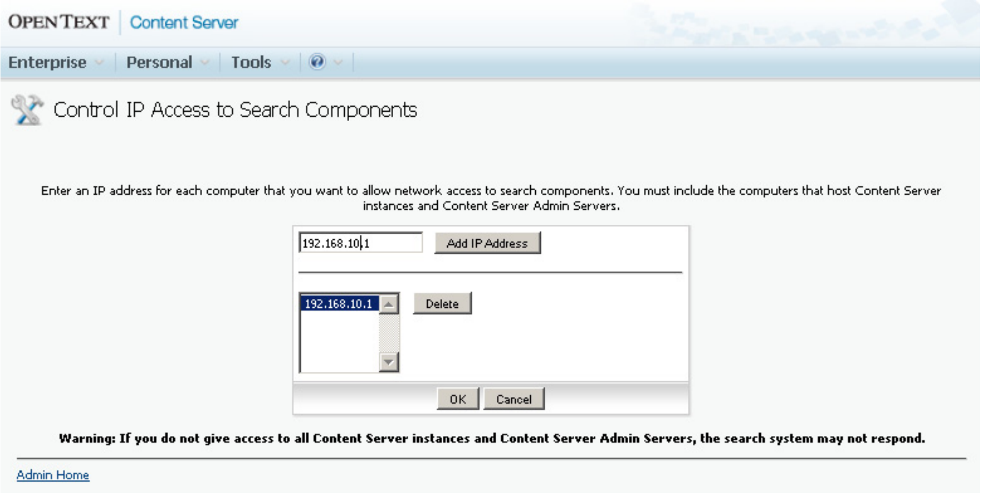
Content Server Administration → Search Administration → Control IP Access to Search Components

EXTERNAL

Some Content Server installations have separate Admin servers and front-end servers. The search and indexing components run as processes on the Admin server. These components communicate with each other and the front-end servers—servers the actual users interact with—using TCP/IP.

Most often, users do not need and are not expected to have direct access to the search components. As such, these components can be secured behind a firewall that only allows access from front-end servers and other Admin servers. In addition to this approach, Content Server can be configured to control the IP Addresses from which the search and index tier will accept requests.

Figure 5



Control IP Access to Search Components

Enter an IP address for each computer that you want to allow network access to search components. You must include the computers that host Content Server instances and Content Server Admin Servers.

192.168.10.1 [Add IP Address]

192.168.10.1 [Delete]

[OK] [Cancel]

Warning: If you do not give access to all Content Server instances and Content Server Admin Servers, the search system may not respond.

Admin Home

Administrators can enter the IP addresses for the computers that host Content Server instances and Content Server Admin servers in this page. This will prevent the search and index services from accepting outside requests, limiting the number of IP addresses that can interact with the services.

DEFAULT SETTING: There are no restrictions enabled; there are no restrictions as to the IP addresses of machines that can interact with the search services.

HTML Page Encoding

Content Server Administration → Server Configuration → Configure Server Parameters

Character Set

XSS

All Content Server deployments should have an explicit Character Set as part of the installation process. Ensure that the Character Set value is appropriate for your deployment.

DEFAULT SETTING: This field is set to `UTF-8` by default.

Auditing Interests

PRIVACY

Content Server Administration → System Administration → Administer Event Auditing → Set Auditing Interests

Content Server offers a comprehensive set of events that can be audited. Administrators should review the list of auditable events according to the organization's security policy. This should set the desired auditing prior to users accessing the system.

Administrators should familiarize themselves with the **Query Audit Log** feature available at **Content Server Administration → System Administration → Administer Event Auditing → Query Audit Log.** Note that the audit log is stored as a table within the relational database and can be configured so that the front-end server connections (maintained as a single DB user) can write to the table but do not have read permissions.

DEFAULT SETTING: See **Appendix B - Default Audit Settings** for a list of items that are audited by default.

Multi-File Output

Content Server Administration → Multi-File Output Administration → General Settings

Temporary Directory Settings

PRIVACY

The temporary directory will store selected content while the server is compressing the files for delivery. This file directory should be secured using file system access controls to ensure that non-authorized users cannot access the temporary files.

DEFAULT SETTING: `<OTHOME>/temp/multifile` is the default directory.

Attachment Options

PRIVACY

This setting controls how attachments are handled in email generated by Content Server. There are three different options. These include:

- **Allow the user to choose** –The user can choose if they wish to send the file or the URL for the document through email
- **Use files only** – The actual file is sent by email.
- **Use URLs only** – The URL to the file is delivered in an email message.

> **NOTE:** Once a document is sent via email, Content Server cannot control the dissemination of the document; and Content Server cannot validate to whom the email message (and the attached document) is being sent.

DEFAULT SETTING: Allow the user to choose is enabled; this allows users to choose either the delivery of actual files or URLs to the files when sending a file through email.

Object Creation

Content Server supports many different object types, from simple documents and containers (like folders) to specialized object types. Some of these object types are used to alter the display of the Content Server user interface, while others provide access to audit data and model business processes. Administrators should evaluate the needs of users and limit privileges to only those users that require the privilege to fulfill their business needs.

Administer Object and Usage Privileges

ASR

Content Server Administration → System Administration → Administer Object and Usage Privileges

Object Type Creation rights and Usage Privileges (access to selected Content Server functionality) can be restricted to specific users and groups.

Select **Restrict** in the Action column to restrict creation of a particular Object Type or Usage Privilege. If the **Edit Restrictions** and **Delete All Restrictions** options are displayed, there are already restrictions in place that can be changed or removed entirely.

Depending on the current settings, administrators may be notified that no users will be able to create these objects until the group is initially populated. Select **OK** when that message is presented.

Administrators can now add users and groups to the corresponding group. If none are added, the only user that will be able to create the object type in question will be the Admin user.

Discussion of Object Type Restriction

Review the following object types and consider restricting those that are not restricted by default:

URL

XSSASR

`URL` objects allow users to create links that can be followed in the Content Server user interface.

- `URL` objects could potentially be used to create Content Server URLs that confuse the user – for example, navigate them to the permissions page for an object. (They cannot be used to create POST events).
- `URL` objects could be used to create links to external sites. The content of the external sites may be malicious. For example, it may present pages that users think are part of the internal system, and may entice them to add confidential information to that site.
- `URL` objects have the potential to change the user interface. A malicious user could create a persistent Cross-Site Scripting (XSS) worm that is embedded on a Content Server page. Users could then be enticed to utilize the `URL` object and become victim of the Cross-Site Scripting worm. Content Server logs the creation of all objects and the user account that was used to create the URL object in question would be logged.

DEFAULT SETTING: `URL` objects are restricted; only the Admin account can create `URL` objects.

Workflow Map

ASRPRIVACY

The creation of a Workflow Map is an advanced activity. As such, it should be restricted to only those users familiar with the business processes that are being automated though the Workflow. A malicious user could craft a Workflow Map that an unwitting user could use. This malicious Workflow Map could distribute documents improperly, perhaps disclosing information inappropriately.

DEFAULT SETTING: Workflow Map objects are **Unrestricted**; all users can create `Workflow Maps`.

Custom View

XSSASR

`Custom Views` can be used to alter the Content Server user interface. `Custom Views` are HTML documents and can carry malicious active scripts. Administrators should consider this when granting the privilege to create `Custom Views` to users.

DEFAULT SETTING: `Custom View` objects are `Restricted`; only the Admin account can create `Custom View` objects.

Workflow Status

PRIVACY

Workflow Status objects allow users to view reports on the status of workflows. Administrators should review the confidential nature of the status of workflows for their organization and restrict the ability to create Workflow Status objects appropriately.

DEFAULT SETTING: Workflow Status objects are **Unrestricted**; all users can create Workflow Status objects.

wantTestArgs setting

PRIVACYASR

To help diagnose issues, the entry `wantTestArgs=TRUE` can be set in the `[options]` section of the `opentext.ini` file. This setting bypasses a number of security configuration items. It should only be used on production systems when all user access is denied—except for trusted staff that are addressing support issues.

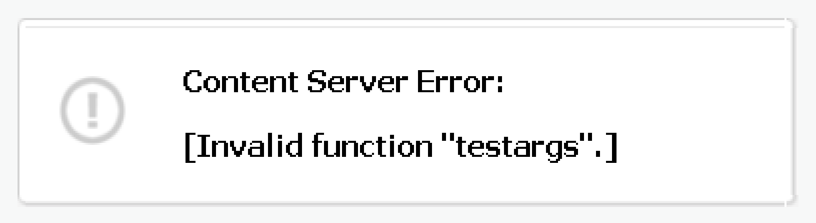
Once the setting has been used to diagnose issues and is no longer needed, it should be removed from the `opentext.ini.` Content Server must then be restarted and a test performed to ensure that the change has been successful.

To test for successful removal, enter:

`http://server_name/OTCS/cs.exe?func=testargs`

(Individual deployments may require modification of the `server_name/OTCS/` portion of the URL).The resulting page should display:

Figure 6



Content Server Error:

[Invalid function "testargs".]

DEFAULT SETTING: The `wantTestArgs` setting is not in the `opentext.ini` file; the `testargs` function is disabled.

Protecting the NextURL Value

XSSCSRF

Content Server is designed to allow users to quickly navigate for information, make content available to others easily and share simple links to content amongst other users. To support these goals, Content Server is “stateless” – which means that a user does not have to go through a preset series of steps to accomplish a task, such as to access content.

However, for some interactions a sequence of events must be maintained. To assist with this situation, the `NextURL` value is often used.

The `NextURL` value is delivered to the user’s browser as part of a response to a request. For example, if a user requests to add a Task List, the response from the server is a page that allows them to define the name for the Task List. The page includes a `NextURL` value. The `NextURL` value is the next logical request (expressed as a URL) to complete the addition of a Task List to Content Server.

The challenge is to protect the `NextURL` value from attackers who want to direct Content Server users to other sites.

This section explains how to use the `checkNextURL`, `cgiDirectory`, `allowedNextURLSites`, and `allowedNextURLPrefixes` options in the `[Security]` section of the `opentext.ini` file to secure the `NextURL` from attack through redirection.

The nomenclature of the checkNextURL feature

To set the `checkNextURL` feature correctly, it is important that administrators understand the names given to the portions of the URL values. The following are two example URLs and their breakdown:

http://my-server/contentmgmt/cs.exe?func=...	
Protocol	http
Server name	my-server
Prefix	contentmgmt
CGI / file	cs.exe
	Appended information such as `?func=…` is not validated.

http://my-server/contentmgmt/corp/cs.exe?func=...

Protocol	http
Server name	my-server
Prefix	contentmgmt/corp
CGI / file	cs.exe
	Appended information such as `?func=`… is not validated.

Enabling Validation

The `checkNextURL` option has two settings. When set to `FALSE` (default), no validation of the `NextURL` parameter is required and all other settings described in this document are ignored. To enable validation of the `NextURL` values, the `checkNextURL` option in the `[Security]` section of the `opentext.ini` file must be set to `TRUE`.

Server Validation

When Content Server receives a request with a `NextURL` value, it determines if the value is an absolute URL or a relative URL. No configuration is required, except to set the `checkNextURL` value to `TRUE.`

Absolute URL

An absolute URL is a URL value that includes the protocol, server name, prefix, and CGI and file values. If the `NextURL` is an absolute URL, the server name portion of the URL is compared to the server name in the request. For example:

Request	http://my-server/livelink/llisapi.dll?func=abc123
`NextURL` value	http://my-server/livelink/llisapi.dll?func=def456

The server portion of the `NextURL` value (`my-server`) in the request is the same as the server value in the `NextURL` (`my-server`) and is valid. The following is an example of a `NextURL` value that does not meet the validation test:

Request	http://my-server/livelink/llisapi.dll?func=abc123
`NextURL` value	http://another-server/livelink/llisapi.dll?func=def456

The server portion of the `NextURL` value (`my-server`) in the request is not the same as the server value in the `NextURL` (`another-server`) and is not valid.

Relative URLs

A relative URL is a URL value that does not include the protocol and server name. Since the server name portion is not present, the server name cannot be evaluated. If the NextURL is a relative URL, the server name portion of the NextURL is not present and cannot be evaluated, as is shown in the following example:

Request	http://my-server/livelink/llisapi.dll?func=abc123
NextURL value	/livelink/llisapi.dll?func=def456

It is important to understand that attacks on NextURLs that are relative URLs will most likely fail. In the following example, the attacker is attempting to redirect the user to /evil-server/.

Request	http://my-server/livelink/llisapi.dll?func=abc123
NextURL value	/evil-server/livelink/llisapi.dll?func=def456

This will fail because the NextURL will be interpreted by Content Server as the URL of

http://my-server/evil-server/livelink/llisapi.dll?func=def456, which will not resolve.

Further Validation

There are 3 options in the [Security] section of the opentext.ini file that are used during the checkNextURL validation process.

cgiDirectory

- The opentext.ini file entry is cgiDirectory=
- The default value is cgi. This is the default name of the directory under <OTHOME> that has the CGI and ISAPI binaries for Content Server.
- Administrators can use this option to set the name of the directory which contains the CGI and ISAPI binaries. The names of the files will be used as valid values for the CGI and file portion of the NextURL. In the following example, the NextURL value would be valid as the llisapi.dll in the CGI / file portion of the URL is included in the list of files found at <OTHOME>/cgi.

Request	`cgiDirectory=cgi` (and the `<OTHOME>/cgi` directory contains the following files) • `livelink` • `cs.exe` • `llisapi.dll` • `llkernel.dll` • `llresources.dll` • `llresourceswin.dll` • `llview1` • `llview.exe` • `wkernel.dll`
`NextURL` value	http://my-server/livelink/llisapi.dll?func=def456

10.5 only

- Administrators should ensure that no unwanted executables are added to the `cgi` directory after deployment as they would be automatically accessible through the `NextURL` value.

allowedNextURLSites

- The `opentext.ini` file entry is `allowedNextURLSites=`
- This option allows the administrator to specify valid binaries in addition to those in `cgiDirectory`. Administrators can specify which CGI and ISAPI binaries are valid.
- Format: `allowedNextURLSites = {'hr.exe', 'design.exe'}`

The following example shows that the `NextURL` value is valid, since the `llisapi.dll` CGI and file portion of the URL is included in the list of files associated with the `allowedNextURLSites` value:

	allowedNextURLSites = {'hr.exe', 'design.exe'}
`NextURL` value	http://other-server/corp-app/hr.exe?func=login

Users should note that the `NextURL` value requires that `other-server` must be added to the `cgiDirectory setting` and `corp-app` must be added to the `allowedNextURLPrefixes` setting.

allowedNextURLPrefixes

- The `opentext.ini` file entry is `allowedNextURLPrefixes=`
- The `checkNextURL` validation checks the prefix value. The `NextURL` can have the same prefix as the initial request or a value from the list of prefixes in the `allowedNextURLPrefixes` setting. This option contains a list of allowable prefix values. This list will be used in addition to the prefix of the current request to test if the `NextURL` is valid. In the following example, the `LES` prefix (as provided by the `allowedNextURLPRefix` setting) and the `livelink` prefix (as provided by the request URL) are both valid:

	allowedNextURLPrefixes = {'/LES/'}
Request	http://my-server/livelink/llisapi.dll?func=abc123
`NextURL` value	http://my-server/LES/llisapi.dll?func=def456

- The default value of the `allowedNextURLPrefixes` is {}. This is NULL, meaning that no prefixes other than the one in the request are allowed.
- Format: `allowedNextURLPrefixes={'/prefix/','/another/prefix/'}`
- Please note the starting and ending / character of each value.

WebReports and ActiveView

Both WebReports and ActiveView are powerful modules that allow for customization within Content Server, without the use of the Content Server IDE. Please note:

- To create WebReport nodes in both **Content Server 10.5 and 16.x**, a valid WebReports license is required.
- To create ActiveView nodes in **Content Server 10.5**, the ActiveView module needs to be installed as an optional module and a valid ActiveView license is required.
- To create ActiveView nodes in **Content Server 16.x**, no additional software or license is required.

These modules can be used to build complex applications directly inside Content Server. WebReports and ActiveViews and the tag system they use are governed by Content Server permissions and security settings.

It is possible for a malicious user to create custom applications using WebReports and ActiveViews that violate security guidelines for web applications, such as including JavaScript code that allows XSS attacks. WebReports and ActiveView should be considered development tools, creators should be considered developers, and WebReport and ActiveView development should be subject to any relevant company security policies. Some recommended practices include the following:

- Provide WebReports and ActiveView creation privileges to approved users only.
- Be aware of which users have privileges to create and edit WebReport and ActiveView nodes.
- Set up a process to peer review or programmatically scan WebReports and ActiveView versions before they go into production.

Object Privileges

Creation of WebReport and ActiveView nodes can be administered in the **Administer Object and Usage Privileges** admin page. As of Content Server 10.5 Update 2015-09, WebReports and ActiveView node creation is restricted by default. Users who require privileges to create these types of nodes will need to be added to the WebReport or ActiveView privilege groups.

WebReport and ActiveView nodes follow standard Content Server permissions structures and any applications built using these modules should be permissioned accordingly.

Security Settings

Manage Trusted Files

A WebReport can be configured to use an external file for a Data Source or for a Destination. This is useful when interacting with other applications as it allows the WebReport to read and write data from a file outside of Content Server without the need for adding the document to Content Server. The **Manage Trusted Files** admin page in the WebReports section allows Administrators to configure whitelists of approved paths to prevent unwanted access to certain files that the Content Server process might have access to (for example, the `opentext.ini` file).

Both lists support simple wildcard usage. Direct paths to approved sources or destinations is not required. For example, using `C:\data\WebReportSources\*` in the **Trusted External Files for Data Sources** whitelist would allow any files within `C:\data\WebReportSources\` or its children to be used as a data source for a WebReport.

DEFAULT SETTING: The whitelist is empty by default.

Development Practices

Preventing XSS vulnerable syntax in a Parameter tag

WebReports uses a tag-based syntax which supports command chaining and can resolve to different values and perform various actions. Developers can create reports and applications using dynamic data within the context of the user running the report.

The `Parameter` data tag allows access to a parameter's value in the request. For example: `[LL_REPTAG_&sortDirection /]` in a WebReport would resolve to the value of the `sortDirection` parameter in the request. This syntax is necessary to pass data from one report to another, as in the case where the WebReport developer needs to prompt the user running the report for some data that would affect the returned result set (for example, prompting for a user to find any outstanding tasks that are assigned to that user).

While the `Parameter` data itself is useful, it must be used in a secure manner to ensure that no XSS vulnerabilities are exposed in a WebReport or ActiveView application. For example, if the `Parameter` value is placed inside an HTML input field or a Javascript block, and the `Parameter` is unvalidated, the resulting syntax would be vulnerable to XSS vulnerabilities.

To demonstrate, consider the following code in a WebReport or ActiveView:

```
<input type="hidden" name="count" value="[LL_REPTAG_&count
/]">
```

In this case, the report would replace the `[LL_REPTAG_&count /]` tag with the value of the `count` parameter in the request. This is vulnerable to XSS, as the `count` value is not validated and could contain HTML syntax to terminate HTML input field early and inject additional HTML tags - including a `<script>` block.

As with other secure coding best practices, validating a Parameter tag is the responsibility to the developer of the WebReport. The developer understands the context of how the parameter is used in the report. There are a number of sub-tags available to the developer to aid in validating the passed values. Some of these sub-tags are listed below. Please refer to the Tag Guide for more details on them as well as the full listing of sub-tags that are available:

- `CHECKURL` – checks a URL for potential XSS vulnerable syntax.
  - Example: `[LL_REPTAG_&nextURL CHECKURL:”” /]`
- `ESCAPEFORJS` – converts a string using the same encoding as the specified Javascript escape function.
  - Example: `[LL_REPTAG_&userName ESCAPEFORJS:HEX /]`
- `INT` – attempts to cast the data to an Integer. This is useful if the parameter value is expected to be an Integer.
  - Example: `[LL_REPTAG_&count INT /]`
- `TODATE` – attempts to cast the data to a Date.
  - Example: `[LL_REPTAG_&startDate TODATE /]`
  - Supports custom date formats as well.

External Elements

Underlying Systems

Content Server uses underlying systems such as operating systems, directories, web servers, and databases. All of these systems should be hardened as per each vendor’s best practices. All third-party software should have the most recent security patch sets and updates applied. It is also advisable to use third-party products for additional protection of the network infrastructure.

The web server environment must have implemented best practices and protection mechanisms such as adequate protocols, cluster management, failover, and filtering of incoming connections.

Ensure Browser Supports Http-Only Property

Content Server utilizes many technologies that are only supported in the recent versions of some browsers. OpenText provides a list of supported browsers in the Content Server Release notes – these can be found on the OpenText Knowledge Centre. For optimal security, Content Server users should only use browser versions that are certified by OpenText for use with Content Server.

A key technology that is found only in supported browsers is the `HttpOnly` configuration option for cookies. This document contains information about the use of the `HttpOnly` configuration option and the vulnerability that it addresses.

DEFAULT SETTING: Content Server Administrators should determine if users require a browser that supports the `Http-Only` property. See also enabling http only cookies in Content Server.

Anti-Virus / Malware Considerations

EXTERNAL

In this section, the term “virus” is used to refer to the various kinds of malware, including worms, Trojan horses, logic bombs, and other invasive pieces of code within corporate or organizational environments.

Administrators need to ensure that OpenText Content Server deployments and related server systems are scanned for viruses on a regular basis.

Administrators should also make every effort to ensure that desktops, workstations, and even portable systems like notebooks have real-time virus protection, and that virus definitions are regularly updated. This could easily be the first line of defense to counter virus threats in your corporate or organizational environments. Administrators should consult their antivirus software vendor’s website for up-to-date information, critical updates, and patches to ensure their corporate or personal virus scanners have the latest fixes to deal with any reported issues.

Antivirus applications can have detrimental effects on application deployments if not configured correctly.

- An antivirus application must be able to read files from the file system. Sometimes, the process of reading the file will “lock” it and prevent other applications from reading from or writing to the file.
- When an antivirus application has detected what it believes to be an infected file, the antivirus application might (depending on configuration) “quarantine” (move and restrict access) the file or delete the file entirely. However, antivirus applications sometimes identify non-malicious files as a virus. As a result, these files can be inadvertently deleted or quarantined. When this happens, important files can be made inaccessible which can prevent services from running correctly or from running at all.

Administrators should be aware that Content Server can be deployed in a variety of configurations. It can be deployed across multiple servers and use a number of operating systems. Administrators can enhance the default services with add-ons and customizations. OpenText Customer Support can assist customers to determine the appropriate antivirus application configuration for their deployment. OpenText recommends that administrators test changes to configuration of antivirus applications prior to deploying them in production.

OpenText Partners have also created modules that can integrate directly with Content Server and an organization’s existing antivirus solutions to block malware and viruses from being uploaded to Content Server. To inquire about these solutions, please contact your Customer Support channel.

Server Antivirus Software Configuration

Database Management Systems

Database management systems (DBMS) may also have their own recommendations and guidelines regarding virus scanning of their application folders. Administrators should consult the latest published documentation by the respective DBMS and virus scanning vendors. When an antivirus application performs a scan on a file, it places a lock on it. A file lock interrupts the normal functioning of a database. To prevent situations such as a database crash or hang, OpenText recommends that the corresponding DBMS files are excluded from antivirus scanning.

Scan timing

OpenText recommends antivirus scanning is performed in “scan-on-write” fashion for files and directories not specified to be omitted from antivirus scans.

Most antivirus applications have three options as to when to a scan of a file is triggered:

- On-demand or scheduled inspection of files in a file system
- Scan-on-write – Files are inspected when they are written to the file system.
- Scan-on-read – Files are inspected when they are read from the file system.

If “on-demand” or scheduled scanning takes place when the system is operating, files may be locked by the antivirus application. If the scan-on-read option is applied to installation directories for components of Content Server, performance will be degraded for some operations.

Scan Folders

OpenText recommends that the following folders are not scanned:

- The Extended File Store (EFS)
- `<OTHOME>/logs`
- `<OTHOME>/temp`
- `<OTHOME>/tmp`
- Folder(s) where the DBMS database and log files are located
- Web server and Upload directory
- Folders used by the Renditions module
- Folders used by XML Import/Export
- Temp folders used by the Operating System
- Search functionality directories. To determine which directories are used by the Search functionality, an administrator can access and open the System Object Volume in the Search Administration section. For each server named in the Admin Servers section, select the Path Management option from the function menu (the down arrow beside the name of each Admin Server). The directories listed in the Partition Location Manager Paths and Process Paths sections should not be scanned by antivirus applications. In a typical deployment these folders are:
  - `<OTHOME>/index`
  - `<OTHOME>/filters`
  - `<OTHOME>/config`
  - `<OTHOME>/cache`

The explanations for omitting these items from scanning are provided below:

- Antivirus applications can cause issues if they are configured to scan the Extended File Store (EFS). The EFS is used by the Content Server component to store content objects like documents and spreadsheets. File locking can make content unavailable when requested by the application.
- Log files are constantly being manipulated and overwritten by Content Server. Scanning with antivirus software that results in files being locked will cause issues with the services. The following directory should not be scanned by antivirus applications due to this issue:
  - `<OTHOME>/logs`

- The temporary file directories used by Content Server should not be scanned by antivirus applications as the files are accessed and updated on a continual basis. Any delay caused by antivirus scanning will have a considerable impact on performance and may cause system instability.
- The Search functionality in Content Server is particularly susceptible to problems caused by antivirus scanning.

Mitigating Malicious File Uploads

Content Server allows users to upload files of any type. It does not modify the content in any way. It is possible that an authorized user could unknowingly upload content that has malicious active scripts or other malicious content.

Upload Directory

The Upload Directory parameter is used to constrain the location from which Content Server will accept documents or files for upload. The folder specified in this field must be accessible to both the web server and the Admin server. OpenText recommends that you specify the full path to the folder in this field.

Securing File Upload

There are configuration options available to further secure the file upload and download aspects of Content Server from untrustworthy users or connections. This approach controls the upload and download of HTML files, which results in the following conditions:

- Users must respond to a **Save As** dialog box.
- Users must rename files from `.bin` back to their respective file extension (HTML, HTM) once they have downloaded the file.

Proper configuration of all other known MIME types results in only HTML and optionally TEXT files being handled in this way.

MIME Type Configuration

The following section describes the configuration required to ensure the correct MIME types. This option ensures that:

- Potentially dangerous file types that could contain active scripting are assigned a MIME type that causes the browser to simply render the contents of the file (for example, `text/plain` uses notepad, `application/octet-stream` forces a Download **Save As** dialog).
- Potentially dangerous file types are not passed to the **View as HTML Page** function.
- Potentially dangerous file types are not handled with the **Open** function, but instead are always downloaded.

Disabling MIME Type Auto-Detection

OpenText Installation Folder / Config / opentext.ini

- You must add a setting to the opentext.ini file to stop the auto-detection of MIME types. Without this setting, CS examines the body of the document and attempts to auto-detect the MIME type, which in turn overrides the MIME type mapping.
- You must add this setting to the general section of the opentext.ini file. `ignoreAutoMimeTypeDetection=TRUE`

MIME Types File

OpenText Installation Folder / Config / MIME.types:

The first step is to associate all potentially harmful file types with a MIME type that the browser does not actively render. A suitable MIME type for this purpose is the `application/octet-stream` type.

Rather than attempt to list all potentially harmful file types, you can exploit the way CS works and the format of the `MIME.types` file to create a white list. This is achieved by placing the MIME type you wish to use as the default at the top of the file and associating it with a safe file extension so that CS also renames the file when downloaded.

Once you have configured the first line, you can proceed to add the MIME type extension mappings for acceptable file types that:

- Do not render inline in the browser in an active format (so "`xml, html, htm, dtd, xsl`" should not be added).
- The user can open using a suitable desktop viewer or application (such as Microsoft Office for Office documents).

A short example `MIME.types` file is shown here:

```
# MIME type to file extension mapping file.
#
# This is a whitespace-separated values file where blank lines
and text
# following "#" is ignored.
#
# Each line is a separate entry with the following format:
# ...

application/octet-stream bin
text/plain txt
application/msword doc
application/pdf pdf
```

Most file types contain the ability to provide dangerous content of one kind or another. The intention of the MIME type file provided by OpenText is to enable interoperability with known applications. You may discover that certain applications and file types are not to be trusted within your environment. Check each entry thoroughly.

Viewable MIME Types

OpenText Installation Folder / Config / opentext.ini:

The viewable MIME types section within the `opentext.ini` file controls which MIME types are not sent to the **View as HTML Page** function.

It is important that this contains the default MIME type (the first line in the `MIME.types` file) along with `text/plain` to ensure they are not displayed inline in a Content Server browser page.

The following example section shows how both `text/plain` and `application/octet-stream` have been added to the configuration:

```
[ViewableMimeTypes]
MimeType_1=image/gif
MimeType_2=image/jpeg
```

```
MimeType_3=text/plain
MimeType_4=application/octet-stream
```

Fetch MIME Types

OpenText Installation Folder / Config / opentext.ini:

The Fetch MIME Types setting controls which MIME types are downloaded (sent with a content-disposition attachment header), rather than just sent to the browser.

Internet Explorer prompts you to render active content when the MIME type is `text/plain` and the content looks like HTML (even if you have the Internet Explorer **Open based on content** setting disabled). Therefore, if you are concerned that users may select **Yes**, or that a malicious user uploads an HTML file and then alters the MIME type (possible using the **Specific** Properties tab on the object), then you may add this MIME type to this configuration section.

```
[FetchMimeTypes]
type1=application/x-msdownload
type2=application/octet-stream
type3=text/plain
```

Validating an Individual File Type

When new MIME types are added, you must validate the configuration by performing the three Content Server view operations:

- **View as Web Page:** For types that can be viewed as HTML, this should open a Content Server page with a frame containing the rendered HTML. For types that cannot be viewed as HTML, the file must be sent to the browser (they are in the Viewable MIME Types configuration).
- **Open:** This operation sends the file to the browser without an attachment content disposition header, therefore not invoking the **Save As** dialog box. For types in the Fetch MIME Types section, the attachment content disposition header is sent causing a **Save As** dialog box.
- **Download:** This operation sends the file to the browser with an attachment content disposition header thus causing a **Save As** dialog box.

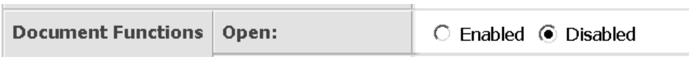
Disable the Open button

For additional security, disable the **Open** button using the options in the Content Server Admin pages:

Content Server Administration -> Server Configuration -> Configure Security Parameters.

```
?func=admin.securityvars
```

Figure 7



Document Functions	Open:	○ Enabled ● Disabled

This forces users to use the **Download** link. However, this disables the **Open** function application-wide for all file types.

You may also configure your client browsers not to offer to open files on download, or instruct users to not open on download.

Appendix A – Functions with Secure Request Token Mechanism

Copying content objects	Editing the list of participants to an object
Creating content objects	Renaming content objects
Deleting content objects	Reserving content objects
Deleting versions of content objects	Unreserving content objects
Editing permissions on content objects	Using the inline text editing system
Moving content objects within Content Server	Editing values of attributes on content objects
Changing the properties (such as MIME type, Nickname) for content objects	Sending links to content objects by email
Adding new versions of content objects	Restoring content objects from the Recycle Bin
Adding permissions to content objects	Renaming a Wiki
Changing the ownership of content objects	Renaming a Community
Applying permissions to subfolders and content objects within those subfolders	Changing properties on Blogs
Zip & Email functionality	Changing properties on Communities
Editing existing user accounts	Changing properties on Forums
Creating new users	

Appendix B – Default Audit Settings

Audit Items - Enabled by Default	
Attributes Changed	Category Added
Category Removed	CD Ordered
Configuration Changed	Copy
Create	Delete
Edit	Failed Log-in Attempt
Function Executed	Generation Created
Log-in	Log-out
Major/Minor Disabled	Major/Minor Enabled
Members Changed	Membership Changed
Move	Owner Changed
Permissions Changed	Project Membership Changed
Provider Retry Deleted	Provider Retry Queued
Provider Retry Queuing Error	Provider Retry Retried
Purge	Release Created
Release Deleted	Rename
Rendition Created	Rendition Deleted
Reserve	Revision Created
Revision Deleted	Shortcut Created
Unreserve	Version Added
Version Control Changed	Version Deleted
Version Locked	Version Opened
Version Promoted	Version Unlocked
View	

Audit Items - Not Enabled by Default	
Content Extraction Failure	Content Extraction Recovery
Data Source Purged	Enterprise Database Re-Extracted
Invalid Session Blocked	Live Report Executed
Log-in Disabled	Print
Provider Changed	Search Statistics Auto-Purged
Search Statistics Purged	Workflow Status Changed
Xml Export	Zip and Download
Zip and E-mail	

Appendix C – Site-Specific Settings

The following are settings that are specific to each Content Server instance:

Option / Configuration	Default Setting
Configuring Security Parameters → Limiting Access to the Administration Pages	Field is left blank, allowing access to the `admin.index` page from any IP address.
Configuring Security Parameters → HTTP-only Cookies	Disabled, therefore authentication cookies will lack the HTTP-Only property.
Configuring Security Parameters → Cookie Encryption Key	The field is empty; the installation directory name is used as the encryption key.
Configuring Security Parameters → Data Encryption Key	The field is empty; the installation directory name is used as the encryption key.
Configuring Security Parameters → Cookie Authentication Information → Client IP Address	255.255.255.255 (Compare Entire IP Address) or ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff/128 (Compare Entire IP Address) (depending upon whether the installation was made on an IPv4 or IPv6 network); Content Server will compare the entire IP address within the cookie and of the source of the request.
Configuring Security Parameters → Cookie Authentication Information → Owner ID	The **Owner ID** checkbox is not selected and the Owner ID is not included in the authentication cookie.
Configuring Security Parameters → Cookie Authentication Information → Password Expiration Date	The **Password Expiration Date** check box is not selected and the **Password Expiration Date** is not included in the authentication cookie.

Option / Configuration	Default Setting
Configuring Security Parameters → Cookie Authentication Information → One-way Encrypted Password	The **One-way Encrypted Password** check box is not selected and the **One-way Encrypted Password** is not included in the authentication cookie.
Configuring Security Parameters → Cookie Authentication Information → Expiration	The **Expire __ minutes after last request** option is selected and number of minutes is set to `30`.
Configuring Security Parameters → Log-in Policies → Disable log-in after ___ failed log-in attempts	**Disable log-in after ___ failed log-in attempts** is enabled, the number of failed logon attempts is set to 5 and the **Send e-mail to the Administrator when log-in is disabled** option is enabled. Content Server will disable accounts automatically when there have been 5 failed logon attempts for that account.
Configuring Security Parameters → Log-in Policies → Disable simultaneous sessions from multiple machines, except for hosts: ______	The checkbox for **Disable simultaneous sessions from multiple machines, except for hosts: ______** is empty, allowing simultaneous sessions from all hosts.
Configuring Security Parameters → Log-in Page Configuration → Disable Browser Autocompletion	**Disable Browser Autocompletion** is enabled, instructing browsers to not allow autocomplete on the logon page.
Configuring Security Parameters → Log-in Page Configuration → Number of Days Password Persists	The field is empty; the password will not persist in the browser for the autocomplete feature.
Configuring Security Parameters → Request Argument Filtering	The field is empty; Content Server will not filter requests.

Option / Configuration	Default Setting
Configuring Security Parameters → Container Size	The checkbox is not selected; this allows the number of items in a container to be displayed.
Configuring Security Parameters → Secure Token Expiration	The **Timeout ___ second after preceding request** option is set to `300` seconds.
Configuring Security Parameters → Secure Request Token Expiration	The field is blank; any server may communicate with the Content Server.
Configuring Security Parameters → Trusted Referring Websites	The field is blank; only the originating Content Server site is a trusted referrer.
Configuring Security Parameters → Document Functions → Open	The **Disabled** radio button is selected; Content Server will not show the **Open** option to users.
Configuring Security Parameters → Document Functions → View as Web Page	The **Enabled** radio button is selected; Content Server will show the **View as Web Page** option to users.
Configuring Security Parameters → Trusted Cross Domains	The **Trusted Cross Domains** box is empty; Content Server will not interfere with the same origin policy restrictions as enforced by the user's browser.
Document Undelete → Configure Autopurge	The **Days Old** field is set to a value of `7`; items are purged after 168 hours (7 x 24 hours)
Document Undelete → Purge Deleted Documents	The **Days Old** field is set to a value of `7`; deleted items that are older than 168 hours (7 x 24 hours) are purged

Option / Configuration	Default Setting
Document Undelete → Immediate Deletion of Documents	The module is installed by default, allowing for the recovery of deleted documents.
Content Server About Page Requiring Authenticated Access	The default is not enabled; all users can access the **About** page.
User Password Settings → Minimum Number of Characters	The value is set to six.
User Password Settings → Passwords Must Contain a Digit	The **Enable** checkbox is selected; passwords require a digit.
User Password Settings → Password Cannot Begin With a Digit	The **Enable** checkbox is not selected; passwords may begin with a digit.
User Password Settings → Changed Password Must Be Different	The **Enable** checkbox is selected; users cannot re-use their previous password when they are prompted to change their password.
User Password Settings → Change Password at First Login	The **Enable** checkbox is selected; users are prompted to change their passwords when they log on for the first time
User Password Settings → Password Expiration	**On** is enabled and the **Days Before Expiration** field is set to `30`; users are notified that their password will expire.
User Password Settings → Days to Prevent Password Reuse	The value is set to `60` (sixty); users cannot re-use passwords previously used in the past 60 days.

Option / Configuration	Default Setting
User Password Settings → Days Required Between Password Changes	The value is set to 0 (zero); users can change their password again immediately after changing their password.
User name Display Control	This option is set to **Log-in ID**; only the user’s log-in id is displayed.
User name Display Control → Append	The checkbox is not selected; Content Server will not add the log-in id to the user name for display. The checkbox is grayed out by default as the default **Display Name Format** is **Log-in ID**.
Configure Access Control → Default Access	None of the checkboxes are selected; no restrictions are in place on the granting of access (access can be granted to groups or individual users), the restoration of Owner Access, Owner Group Access or Public Access privileges.
Configure Access Control → Moving Items across Workspaces → Always inherit the permissions from target destination	The checkbox is not selected; the original permissions of the document are maintained when it is moved and the permissions of the target destination are not applied.
Notifications Administration → Configure Notification → Enable Notifications	The **Enable** radio button is selected; Notifications are sent.
Notifications Administration → Configure Notification → Notification Schedule(s)	**Default Notification Schedule 1**, **Default Notification Schedule 2** and **Default Notification Schedule 3** are all set to send Notifications from 9:00 A.M. to 4:00 P.M. on the hour (according to the server’s time) from Monday to Friday (according to the server’s date).

Option / Configuration	Default Setting
Notifications Administration → Configure Scheduled Activities → Expire Passwords	The **Disable** radio button is selected; no monitoring of expiration of passwords will occur.
Notifications Administration → Configure Scheduled Activities → Monitor Password Expiration	The **Disable** radio button is selected; no monitoring of password expiration will occur.
Notifications Administration → Configure Scheduled Activities → Failed Log-in Notification	The **Disable** radio button is selected; no notification of failed log on attempts will occur.
Logging → Debug & Logging → Content Server Debug Level	The **Content Server Debug Level** is set to `0` (zero); only errors are noted in the logs.
Logging → Debug & Logging → Log Connections	This checkbox is not selected; connection information is not logged.
Logging → Debug & Logging → Log Content Server Timings	Enabled; Content Server timings will be recorded when the **Debug Level** is greater than `0` (zero).
Logging → Debug & Logging → Log File	Logs are created in the `<OTHOME>/logs/ admserv.log` file for the OTAdmin (Admin Server).
Logging → Debug & Logging → Log Level	**Log Level** is set to `1` (one) which will only log errors of the Content Server Admin Server.

Option / Configuration	Default Setting
Control IP Access to Search Components	There are no restrictions enabled; there are no restrictions as to the IP addresses of machines that can interact with the search services.
HTML Page Encoding → Character Set	This field is set to `UTF-8` by default.
Auditing Interests	See Appendix B - Default Audit Settings for a list of items that are audited by default.
Multi-File Output	**Allow the user to choose** is enabled; this allows users to choose either the delivery of actual files or URLs to the files when sending a file through email.
Object Creation → Administer Object and Usage Privileges → URL	URL objects are restricted; only the Admin account can create URL objects.
Object Creation → Administer Object and Usage Privileges → Workflow Map	Workflow Map objects are unrestricted; all users can create Workflow Maps.
Object Creation → Administer Object and Usage Privileges → Custom View	Custom View objects are restricted; only the Admin account can create Custom View objects.
Object Creation → Administer Object and Usage Privileges → Workflow Status	Workflow Status objects are unrestricted; all users can create Workflow Status objects.
wantTestArgs setting	The `wantTestArgs` setting is not in the `opentext.ini` file; the `testargs` function is disabled.

Option / Configuration	Default Setting
Ensure Browser Supports Http-Only Property	

Appendix D – Securing Content Server Services

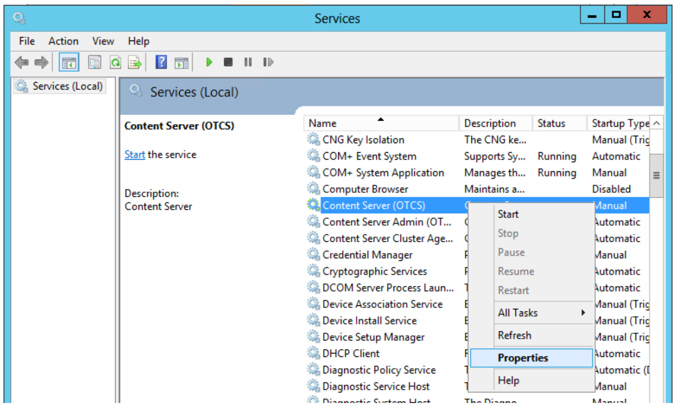
This appendix provides detailed steps for securing Content Server Services. The directions and screen images are on a Windows 2012 system. The same process is applicable to Windows 2008 however there are some differences in dialogs and screens.

Create OTCS User and Set the Content Server Services Permissions

Create the OTCS user on all Windows 2012 R2 servers. Assign full permissions to the `OPENTEXT`, and `Index` folders. For the `EFS` folder, set it up as a share (e.g. `\\<servername>\efs`) and ensure the OTCS user has full permissions to the `upload` folder and also to the `EFS` as well on the database server.

1. Right-click the Content Server service and then click **Properties**.

Figure 8



Content Server (OTCS)

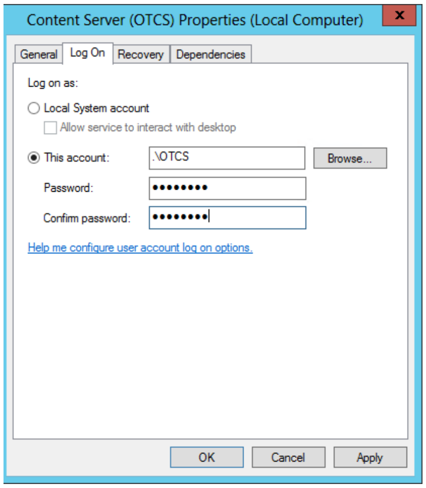
Start the service

Description:
Content Server

Name	Description	Status	Startup Type
CNG Key Isolation	The CNG ke...		Manual (Trig
COM+ Event System	Supports Sy...	Running	Automatic
COM+ System Application	Manages th...	Running	Manual
Computer Browser	Maintains a...		Disabled
Content Server (OTCS)	C		Manual
Content Server Admin (OT...	C		Automatic
Content Server Cluster Age...	C		Automatic
Credential Manager	F		Manual
Cryptographic Services	F		Automatic
DCOM Server Process Laun...	T		Automatic
Device Association Service	E		Manual (Trig
Device Install Service	E		Manual (Trig
Device Setup Manager	E		Manual (Trig
DHCP Client	F		Automatic
Diagnostic Policy Service	T		Automatic (I
Diagnostic Service Host	T		Manual
Diagnostic System Host	The Diagno...		Manual

2. Select the account for Content Server to run as, enter and confirm the password for the account, click **Apply**, and then click **OK**.

Figure 9



Content Server (OTCS) Properties (Local Computer)
General
Log On
Recovery
Dependencies
Browse...
Help me configure user account log on options.
OK
Cancel
Apply

Log on as:

○ Local System account

□ Allow service to interact with desktop

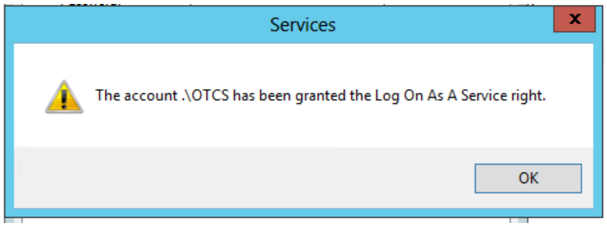
● This account: .\OTCS

Password: ••••••••

Confirm password: ••••••••

3. Click **OK**.

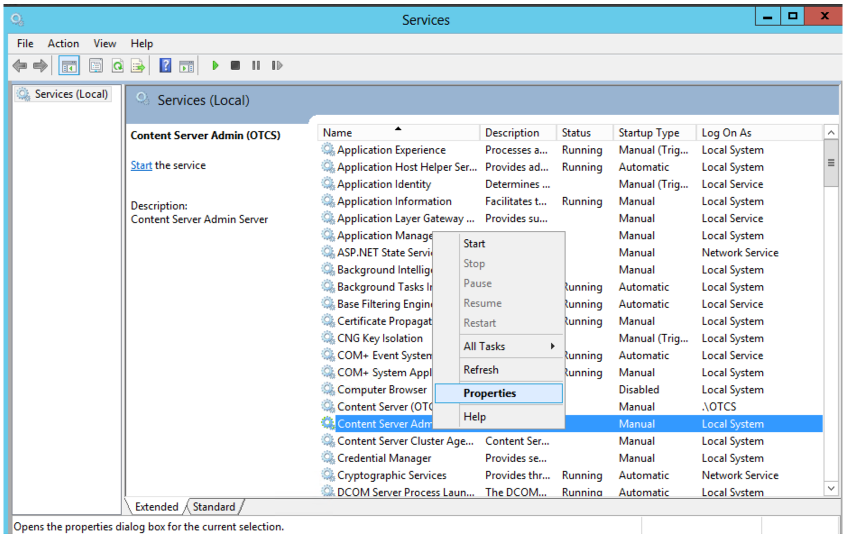
Figure 10



The account .\OTCS has been granted the Log On As A Service right.

4. Repeat *steps 1-3* for the Content Server Admin service and the Content Server Cluster Agent service.

Figure 11



Content Server Admin (OTCS)

Start the service

Description:
Content Server Admin Server

Name	Description	Status	Startup Type	Log On As
Application Experience	Processes a...	Running	Manual (Trig...	Local System
Application Host Helper Ser...	Provides ad...	Running	Automatic	Local System
Application Identity	Determines ...		Manual (Trig...	Local Service
Application Information	Facilitates t...	Running	Manual	Local System
Application Layer Gateway ...	Provides su...		Manual	Local Service
Application Manage			Manual	Local System
ASP.NET State Servi			Manual	Network Service
Background Intellig			Manual	Local System
Background Tasks I		Running	Automatic	Local System
Base Filtering Engin		Running	Automatic	Local Service
Certificate Propagat		Running	Manual	Local System
CNG Key Isolation			Manual (Trig...	Local System
COM+ Event Systen		Running	Automatic	Local Service
COM+ System Appl		Running	Manual	Local System
Computer Browser			Disabled	Local System
Content Server (OTC			Manual	.\OTCS
Content Server Adm			Manual	Local System
Content Server Cluster Age...	Content Ser...		Manual	Local System
Credential Manager	Provides se...		Manual	Local System
Cryptographic Services	Provides thr...	Running	Automatic	Network Service
DCOM Server Process Laun...	The DCOM...	Running	Automatic	Local System

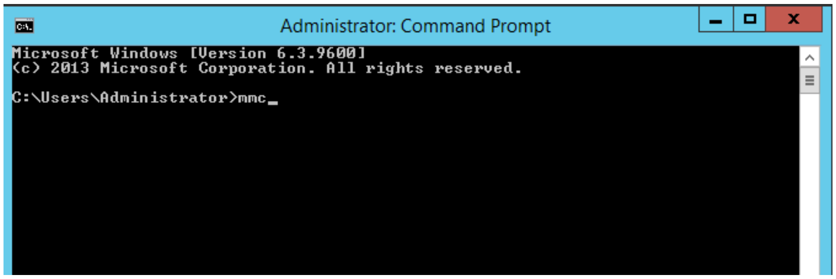
Opens the properties dialog box for the current selection.

Create OTCS Security Template

With the Content Server services assigned to the OTCS user, the next step is to create a security template to control the minimum permissions the OTCS user will require.

1. Launch the Command Prompt and type **mmc**, and then press **ENTER**.

Figure 12

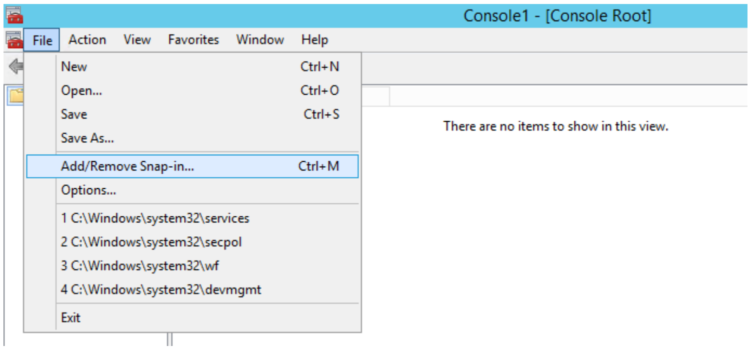


```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>mmc_
```

2. Click **File** > **Add/Remove Snap-In**.

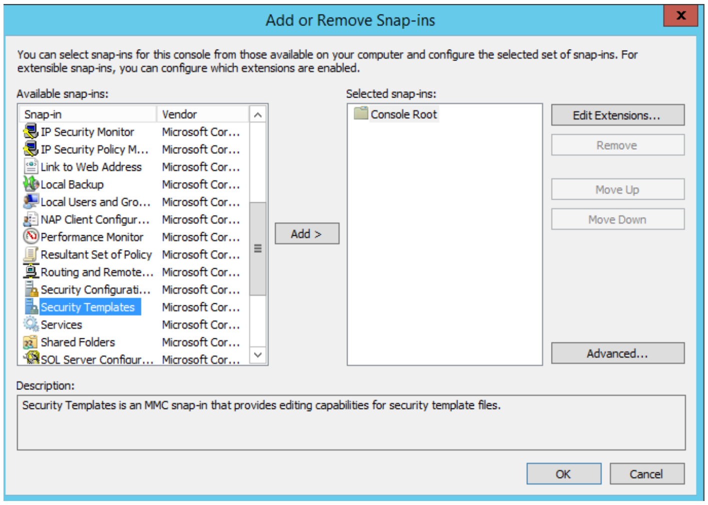
Figure 13


Console1 - [Console Root]
File
Action
View
Favorites
Window
Help
New Ctrl+N
Open... Ctrl+O
Save Ctrl+S
Save As...
Add/Remove Snap-in... Ctrl+M
Options...
1 C:\Windows\system32\services
2 C:\Windows\system32\secpol
3 C:\Windows\system32\wf
4 C:\Windows\system32\devmgmt
Exit

There are no items to show in this view.

3. From the **Available snap-ins,** select **Security Templates** and then click **Add**.

Figure 14



You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.

Snap-in	Vendor
IP Security Monitor	Microsoft Cor...
IP Security Policy M...	Microsoft Cor...
Link to Web Address	Microsoft Cor...
Local Backup	Microsoft Cor...
Local Users and Gro...	Microsoft Cor...
NAP Client Configur...	Microsoft Cor...
Performance Monitor	Microsoft Cor...
Resultant Set of Policy	Microsoft Cor...
Routing and Remote...	Microsoft Cor...
Security Configurati...	Microsoft Cor...
Security Templates	Microsoft Cor...
Services	Microsoft Cor...
Shared Folders	Microsoft Cor...
SQL Server Configur...	Microsoft Cor...

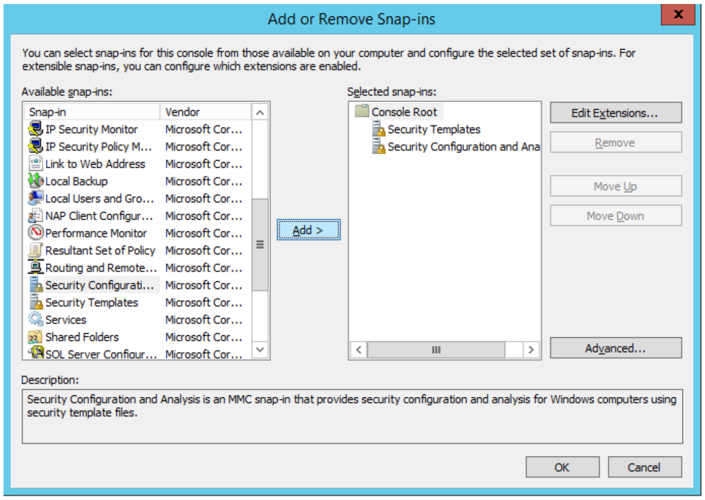
Console Root

Description:

Security Templates is an MMC snap-in that provides editing capabilities for security template files.

4. Next, select **Security Configuration and Analysis,** click **Add**, and then click **OK**.

Figure 15



You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.

Snap-in	Vendor
IP Security Monitor	Microsoft Cor...
IP Security Policy M...	Microsoft Cor...
Link to Web Address	Microsoft Cor...
Local Backup	Microsoft Cor...
Local Users and Gro...	Microsoft Cor...
NAP Client Configur...	Microsoft Cor...
Performance Monitor	Microsoft Cor...
Resultant Set of Policy	Microsoft Cor...
Routing and Remote...	Microsoft Cor...
Security Configurati...	Microsoft Cor...
Security Templates	Microsoft Cor...
Services	Microsoft Cor...
Shared Folders	Microsoft Cor...
SQL Server Configur...	Microsoft Cor...

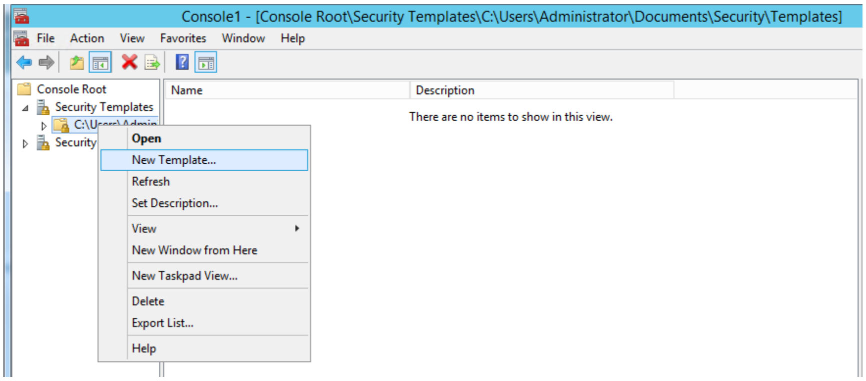
Console Root
Security Templates
Security Configuration and Ana

Description:

Security Configuration and Analysis is an MMC snap-in that provides security configuration and analysis for Windows computers using security template files.

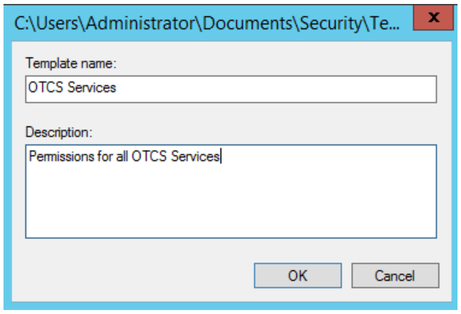
5. Open the **Security Templates**, right-click one level down, and then click **New Template**.

Figure 16



6. Enter a name for the template (for example `OTCS Services`) and a description.

Figure 17

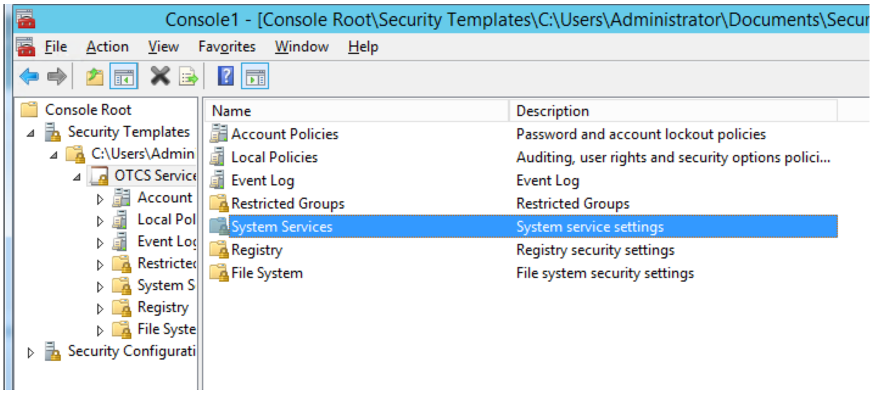


Template name: OTCS Services

Description: Permissions for all OTCS Services

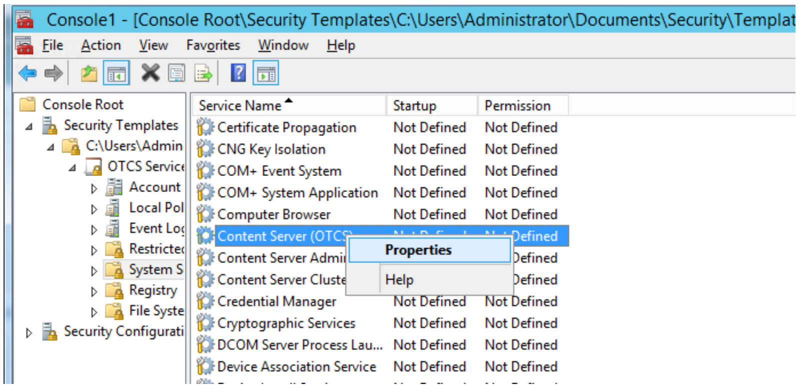
7. Go down one level under **OTCS Services** and double-click **System Services**.

Figure 18



Name	Description
Account Policies	Password and account lockout policies
Local Policies	Auditing, user rights and security options polici...
Event Log	Event Log
Restricted Groups	Restricted Groups
System Services	System service settings
Registry	Registry security settings
File System	File system security settings

8. Right-click **Content Server (OTCS)** service and then click **Properties**.



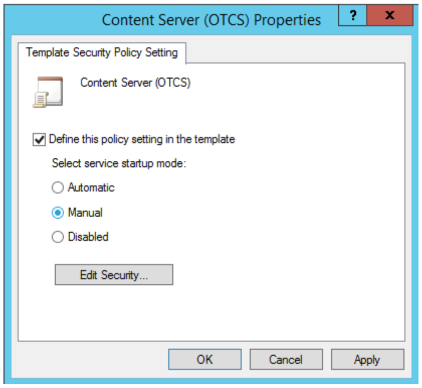
Console1 - [Console Root\Security Templates\C:\Users\Administrator\Documents\Security\Templat

- Console Root
  - Security Templates
    - C:\Users\Admin
      - OTCS Service
        - Account
        - Local Pol
        - Event Log
        - Restricted
        - System S
        - Registry
        - File Syste
  - Security Configurati

Service Name	Startup	Permission
Certificate Propagation	Not Defined	Not Defined
CNG Key Isolation	Not Defined	Not Defined
COM+ Event System	Not Defined	Not Defined
COM+ System Application	Not Defined	Not Defined
Computer Browser	Not Defined	Not Defined
Content Server (OTCS	Not Defined	Not Defined
Content Server Admi		Defined
Content Server Cluste		Defined
Credential Manager	Not Defined	Not Defined
Cryptographic Services	Not Defined	Not Defined
DCOM Server Process Lau...	Not Defined	Not Defined
Device Association Service	Not Defined	Not Defined

Figure 19

9. Select **Define this policy setting in the template** and **Manual**, and then click **Edit Security**.



Content Server (OTCS) Properties

Template Security Policy Setting

Content Server (OTCS)

☑ Define this policy setting in the template

Select service startup mode:

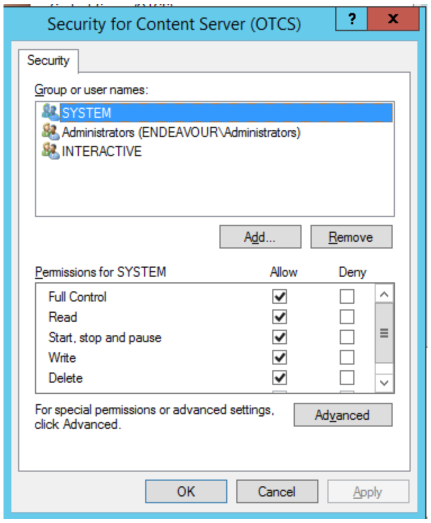
○ Automatic

● Manual

○ Disabled

Figure 20

10. Click **Add**.



Security for Content Server (OTCS)

Security

Group or user names:

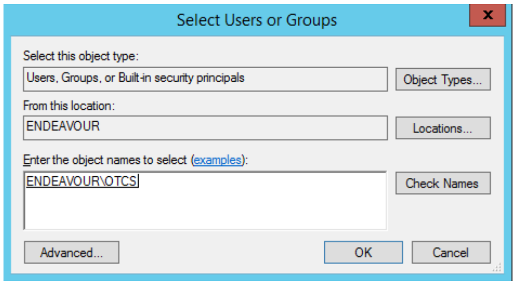
- SYSTEM
- Administrators (ENDEAVOUR\Administrators)
- INTERACTIVE

Permissions for SYSTEM	Allow	Deny
Full Control	☑	□
Read	☑	□
Start, stop and pause	☑	□
Write	☑	□
Delete	☑	□

For special permissions or advanced settings, click Advanced.

Figure 21

11. Type in the `OTCS` user name and click **Check Names.** Once the actual user name is populated, click **OK**.



Select Users or Groups

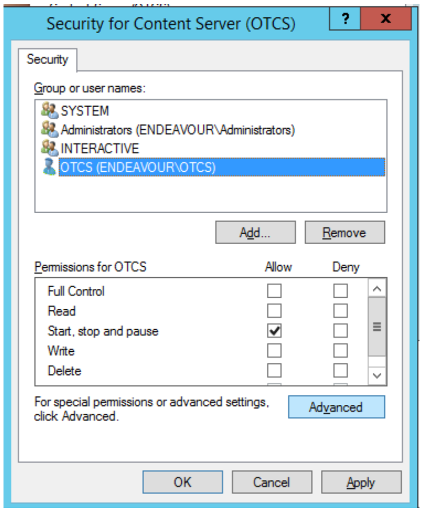
Select this object type:
Users, Groups, or Built-in security principals

From this location:
ENDEAVOUR

Enter the object names to select (examples):
ENDEAVOUR\OTCS

Figure 22

12. With the **OTCS** user selected, click **Advanced**.



Security for Content Server (OTCS)

Security

Group or user names:

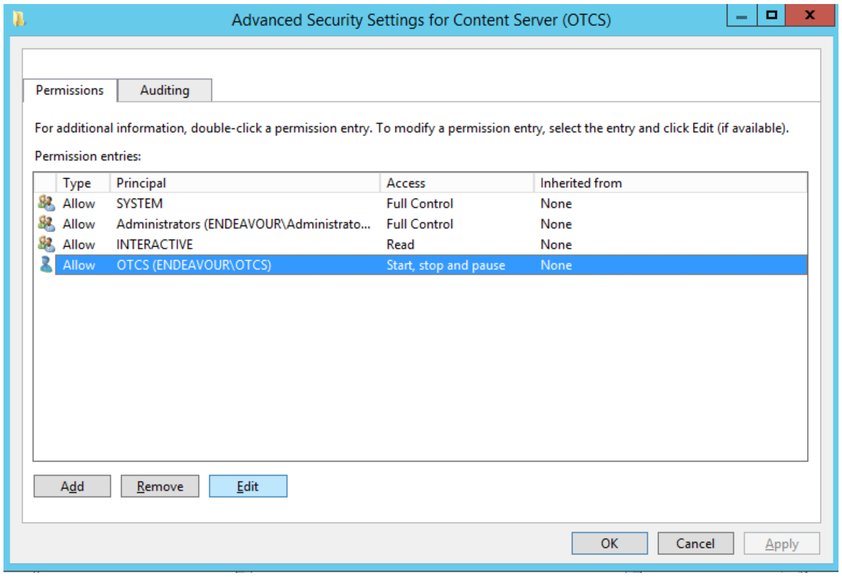
- SYSTEM
- Administrators (ENDEAVOUR\Administrators)
- INTERACTIVE
- OTCS (ENDEAVOUR\OTCS)

Permissions for OTCS	Allow	Deny
Full Control	□	□
Read	□	□
Start, stop and pause	☑	□
Write	□	□
Delete	□	□

For special permissions or advanced settings, click Advanced.

Figure 23

13. Select the **OTCS** user and click **Edit**.



Advanced Security Settings for Content Server (OTCS)

Permissions | Auditing

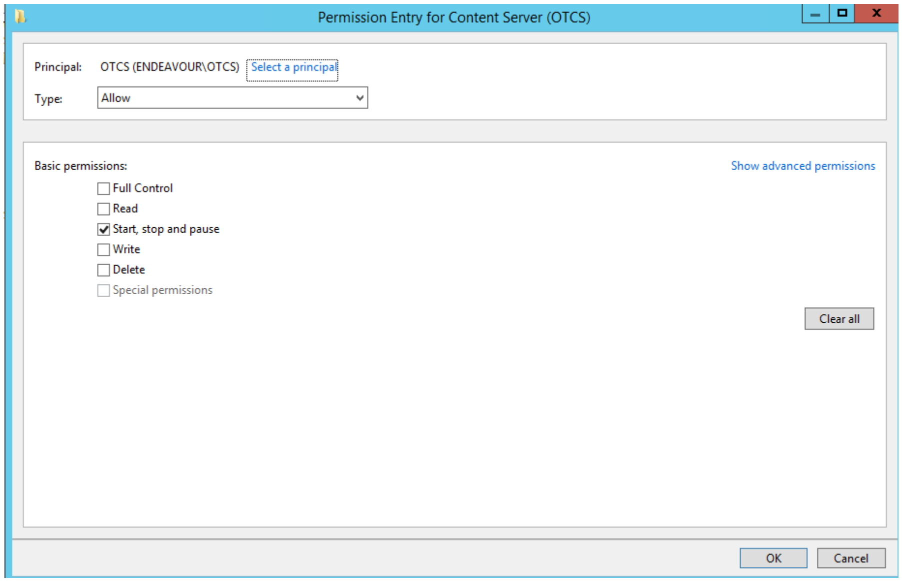
For additional information, double-click a permission entry. To modify a permission entry, select the entry and click Edit (if available).

Permission entries:

Type	Principal	Access	Inherited from
Allow	SYSTEM	Full Control	None
Allow	Administrators (ENDEAVOUR\Administrato...	Full Control	None
Allow	INTERACTIVE	Read	None
Allow	OTCS (ENDEAVOUR\OTCS)	Start, stop and pause	None

Figure 24

14. Click **Show advanced permissions**.



Permission Entry for Content Server (OTCS)

Principal: OTCS (ENDEAVOUR\OTCS) Select a principal

Type: Allow

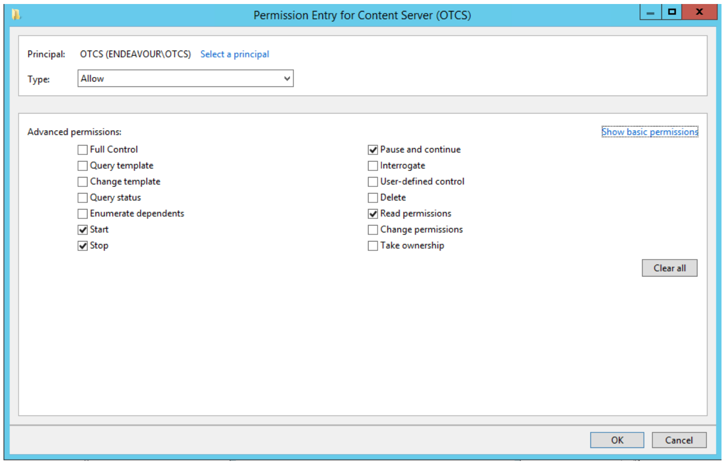
Basic permissions:

Show advanced permissions

□ Full Control
□ Read
☑ Start, stop and pause
□ Write
□ Delete
□ Special permissions

Figure 25

15. Click **Clear All**.



Permission Entry for Content Server (OTCS)

Principal: OTCS (ENDEAVOUR\OTCS) Select a principal

Type: Allow

Advanced permissions:

Show basic permissions

□ Full Control
□ Query template
□ Change template
□ Query status
□ Enumerate dependents
☑ Start
☑ Stop

☑ Pause and continue
□ Interrogate
□ User-defined control
□ Delete
☑ Read permissions
□ Change permissions
□ Take ownership

Figure 26

16. Grant the **OTCS** user account the following permissions:
    - **Query template**
    - **Change template**
    - **Query status**
    - **Start**
    - **Stop**
    - **Pause and continue**
    - **Interrogate**

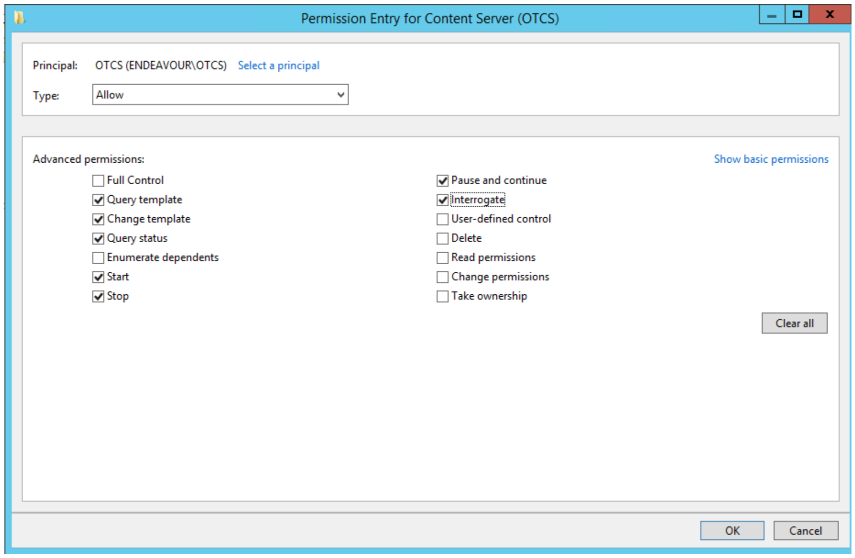


Figure 27

Permission Entry for Content Server (OTCS)

Principal: OTCS (ENDEAVOUR\OTCS) Select a principal

Type: Allow

Advanced permissions:

☐ Full Control
☑ Query template
☑ Change template
☑ Query status
☐ Enumerate dependents
☑ Start
☑ Stop
☑ Pause and continue
☑ Interrogate
☐ User-defined control
☐ Delete
☐ Read permissions
☐ Change permissions
☐ Take ownership

…and then Click **OK**.

17. Click **Apply** and **OK**.

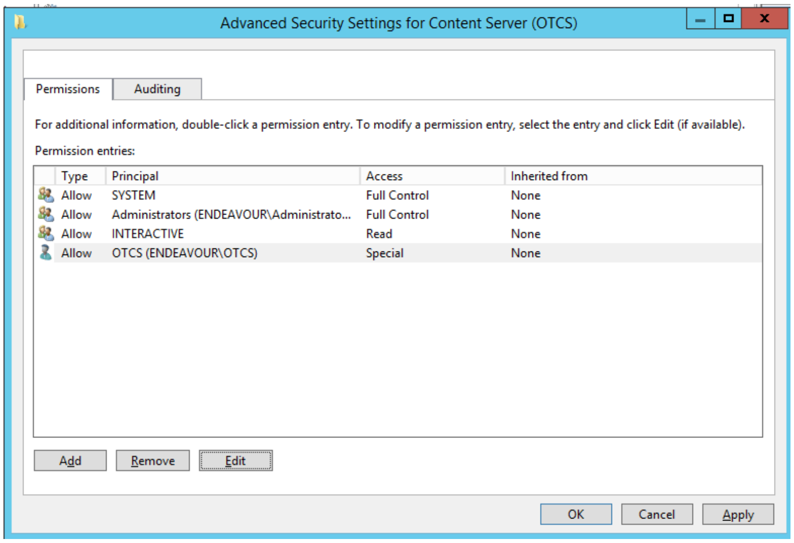


Figure 28

Advanced Security Settings for Content Server (OTCS)

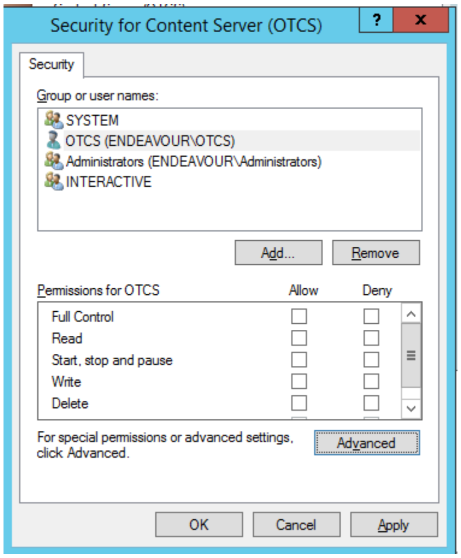
For additional information, double-click a permission entry. To modify a permission entry, select the entry and click Edit (if available).

Permission entries:

Type	Principal	Access	Inherited from
Allow	SYSTEM	Full Control	None
Allow	Administrators (ENDEAVOUR\Administrato...	Full Control	None
Allow	INTERACTIVE	Read	None
Allow	OTCS (ENDEAVOUR\OTCS)	Special	None

18. Click **Apply** and **OK**.

Figure 29



Group or user names:

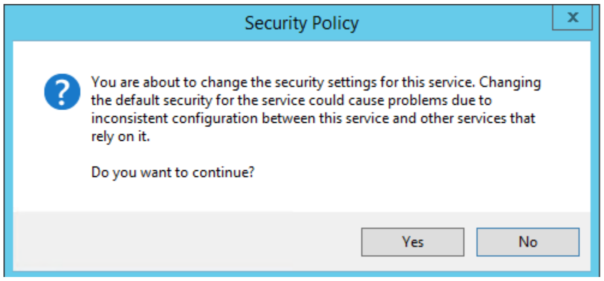
- SYSTEM
- OTCS (ENDEAVOUR\OTCS)
- Administrators (ENDEAVOUR\Administrators)
- INTERACTIVE

Permissions for OTCS	Allow	Deny
Full Control	□	□
Read	□	□
Start, stop and pause	□	□
Write	□	□
Delete	□	□

For special permissions or advanced settings, click Advanced.

19. Click **Yes**.

Figure 30

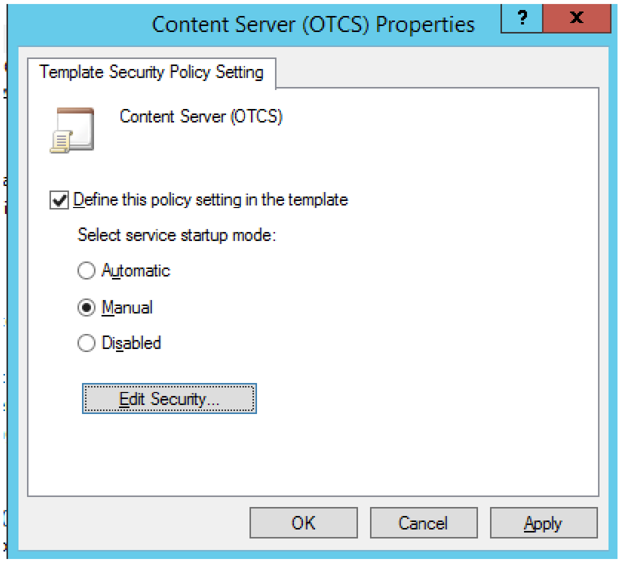


You are about to change the security settings for this service. Changing the default security for the service could cause problems due to inconsistent configuration between this service and other services that rely on it.

Do you want to continue?

20. Click **Apply** and **OK**.

Figure 31


Content Server (OTCS) Properties
?
x
Template Security Policy Setting
Edit Security...
OK
Cancel
Apply

Content Server (OTCS)

☑ Define this policy setting in the template

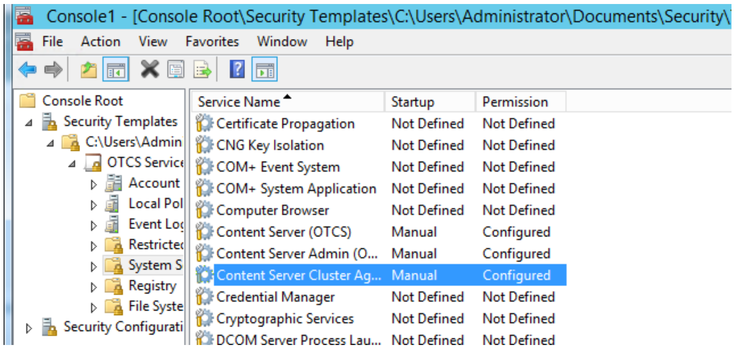
Select service startup mode:

○ Automatic

● Manual

○ Disabled

21. Repeat these same steps for the ***Content Server Admin (OTCS)*** service and the ***Content Server Cluster Agent (OTCS)*** service.

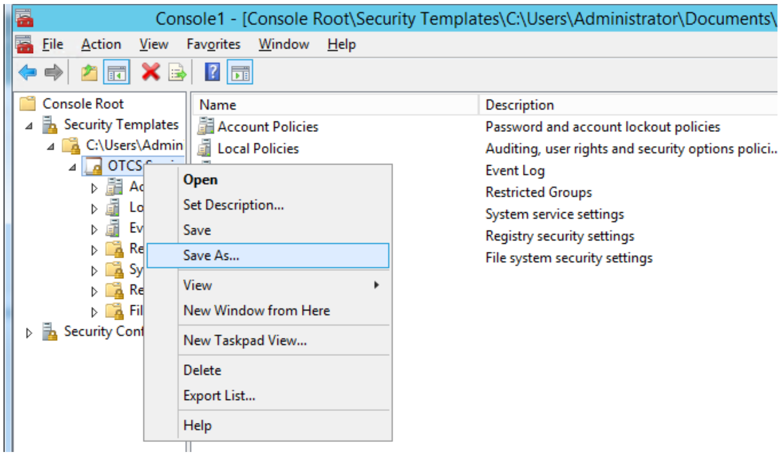


Console1 - [Console Root\Security Templates\C:\Users\Administrator\Documents\Security\

Service Name	Startup	Permission
Certificate Propagation	Not Defined	Not Defined
CNG Key Isolation	Not Defined	Not Defined
COM+ Event System	Not Defined	Not Defined
COM+ System Application	Not Defined	Not Defined
Computer Browser	Not Defined	Not Defined
Content Server (OTCS)	Manual	Configured
Content Server Admin (O...	Manual	Configured
Content Server Cluster Ag...	Manual	Configured
Credential Manager	Not Defined	Not Defined
Cryptographic Services	Not Defined	Not Defined
DCOM Server Process Lau...	Not Defined	Not Defined

Figure 32

22. Right-click **OTCS Services** and then click **Save As**.

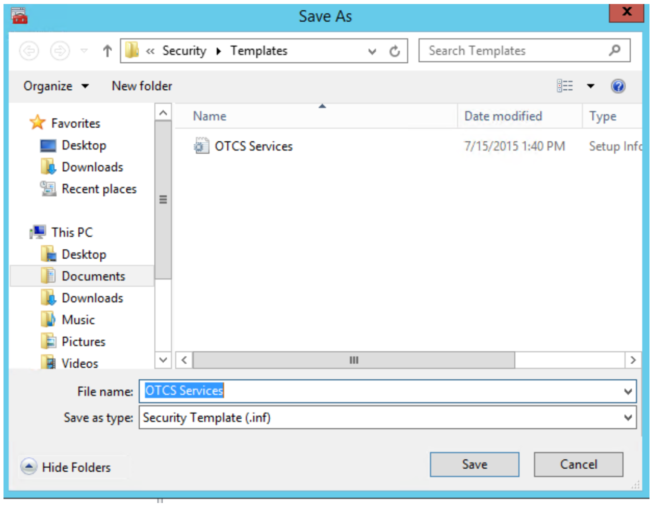


Console1 - [Console Root\Security Templates\C:\Users\Administrator\Documents\

Name	Description
Account Policies	Password and account lockout policies
Local Policies	Auditing, user rights and security options polici..
	Event Log
	Restricted Groups
	System service settings
	Registry security settings
	File system security settings

Figure 33

23. Click **Save**.



Save As

Name	Date modified	Type
OTCS Services	7/15/2015 1:40 PM	Setup Infc

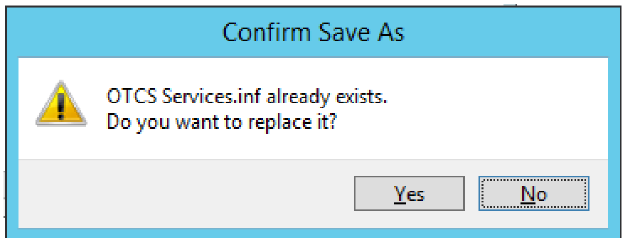
File name: OTCS Services

Save as type: Security Template (.inf)

Figure 34

24. Click **Yes**.

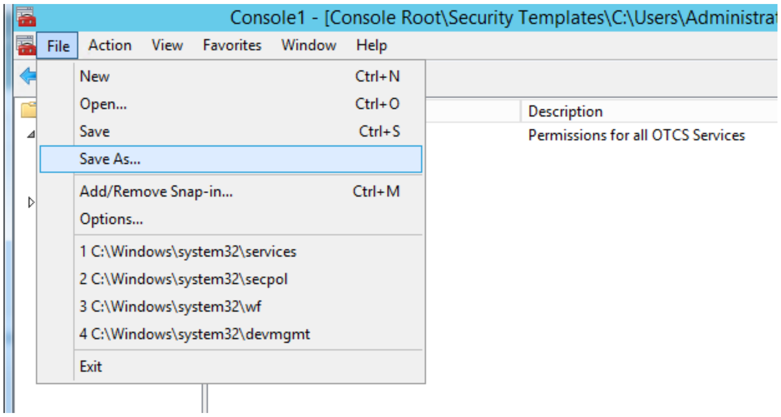
Figure 35



OTCS Services.inf already exists.
Do you want to replace it?

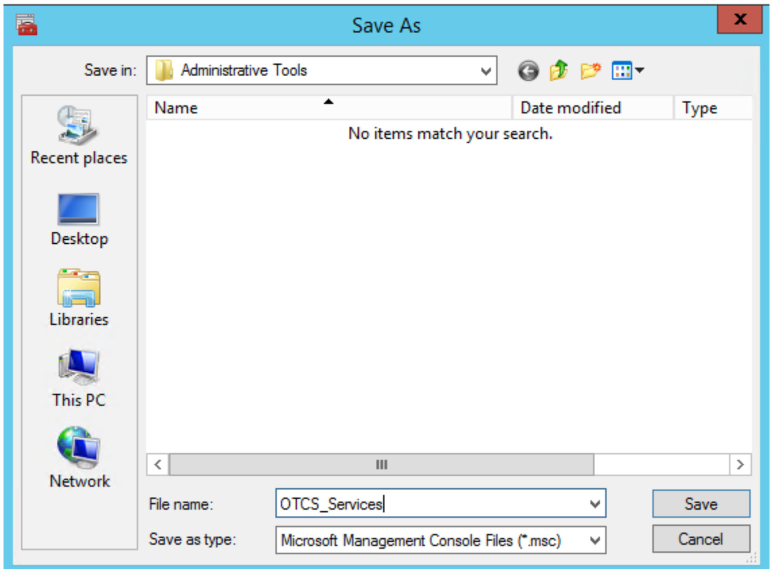
25. Once complete, click **File** > **Save As**.

Figure 36


Console1 - [Console Root\Security Templates\C:\Users\Administrat
File
Action
View
Favorites
Window
Help
New Ctrl+N
Open... Ctrl+O
Save Ctrl+S
Save As...
Add/Remove Snap-in... Ctrl+M
Options...
1 C:\Windows\system32\services
2 C:\Windows\system32\secpol
3 C:\Windows\system32\wf
4 C:\Windows\system32\devmgmt
Exit
Description
Permissions for all OTCS Services

26. Enter an appropriate name for the console configuration (e.g. `OTCS_Services`).

Figure 37



Save in: Administrative Tools

No items match your search.

File name: OTCS_Services

Save as type: Microsoft Management Console Files (*.msc)

Apply the Security Configuration

1. Right-click **Security Configuration and Analysis** and then click **Open Database**.

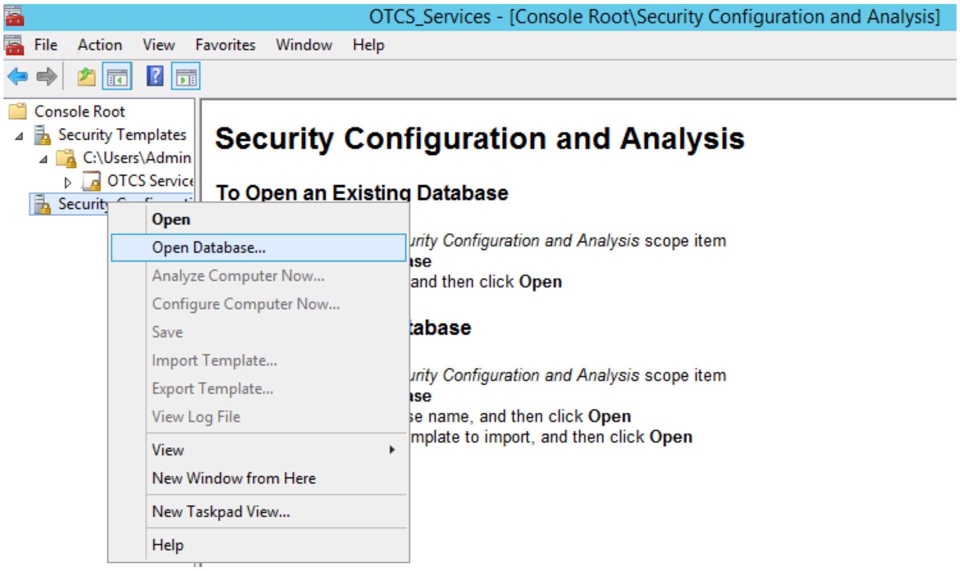


Figure 38

OTCS_Services - [Console Root\Security Configuration and Analysis]

Security Configuration and Analysis

To Open an Existing Database

urity Configuration and Analysis scope item
ase
and then click **Open**

abase

urity Configuration and Analysis scope item
ase
e name, and then click **Open**
mplate to import, and then click **Open**

2. Assign a name to the database (for example, `OTCS_Services`) and click **Open**.

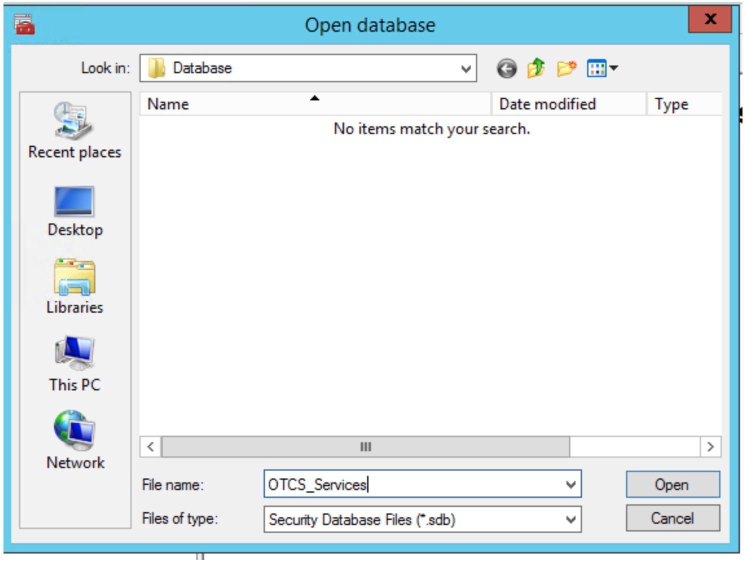


Figure 39

Open database

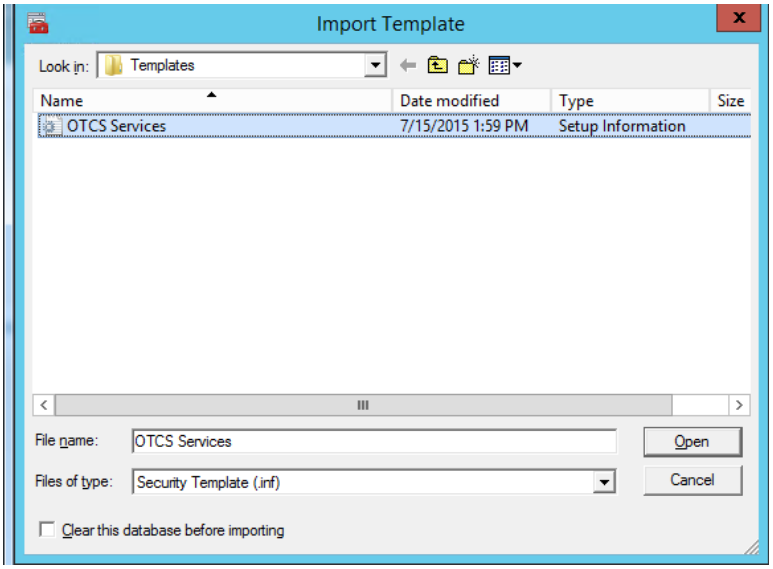
Look in: Database

No items match your search.

File name: OTCS_Services

Files of type: Security Database Files (*.sdb)

3. Select the `OTCS Services.inf` file for import. Click **Open**.



Import Template

Look in: Templates

Name	Date modified	Type	Size
OTCS Services	7/15/2015 1:59 PM	Setup Information	

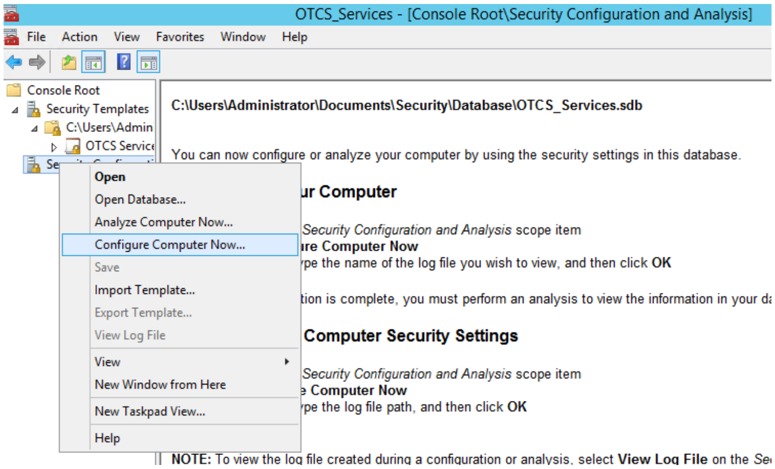
File name: OTCS Services

Files of type: Security Template (.inf)

□ Clear this database before importing

Figure 40

4. Right-click **Security Configuration and Analysis** and click **Configure Computer Now**.



OTCS_Services - [Console Root\Security Configuration and Analysis]

C:\Users\Administrator\Documents\Security\Database\OTCS_Services.sdb

You can now configure or analyze your computer by using the security settings in this database.

ur Computer

Security Configuration and Analysis scope item

ure Computer Now

ype the name of the log file you wish to view, and then click **OK**

tion is complete, you must perform an analysis to view the information in your da

Computer Security Settings

Security Configuration and Analysis scope item

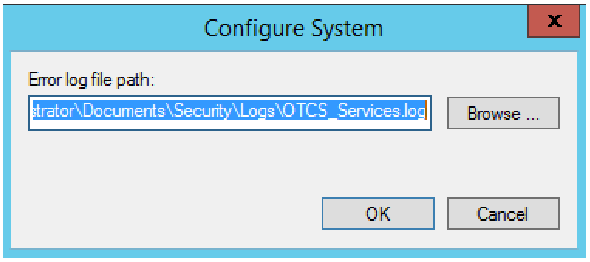
e Computer Now

ype the log file path, and then click **OK**

NOTE: To view the log file created during a configuration or analysis, select **View Log File** on the *Se*

Figure 41

5. Click **OK** for the log file location.



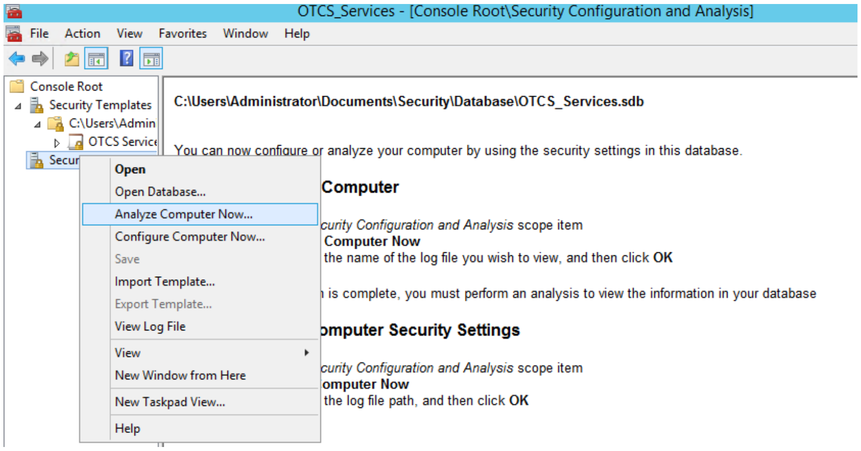
Configure System

Error log file path: strator\Documents\Security\Logs\OTCS_Services.log

Figure 42

6. Next, right-click **Security Configuration and Analysis** and then click **Analyze Computer Now**.

Figure 43



C:\Users\Administrator\Documents\Security\Database\OTCS_Services.sdb

You can now configure or analyze your computer by using the security settings in this database.

Computer

curity Configuration and Analysis scope item
Computer Now
the name of the log file you wish to view, and then click **OK**

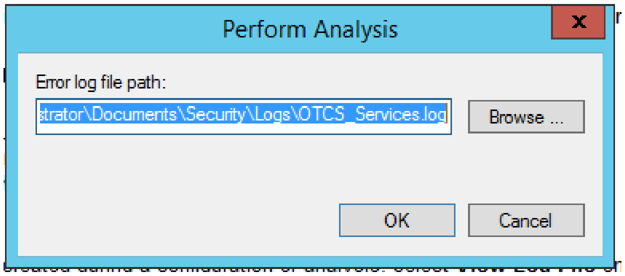
is complete, you must perform an analysis to view the information in your database

omputer Security Settings

curity Configuration and Analysis scope item
omputer Now
the log file path, and then click **OK**

7. Click **OK** for the log file location.

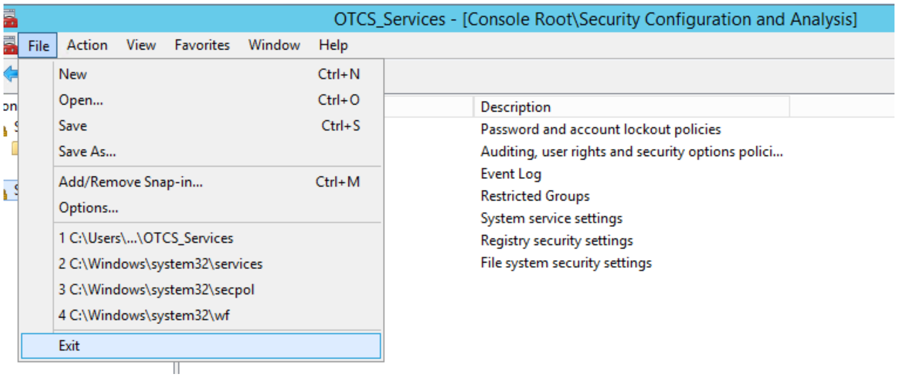
Figure 44



Error log file path:
strator\Documents\Security\Logs\OTCS_Services.log

8. Click **File** and then click **Exit**.

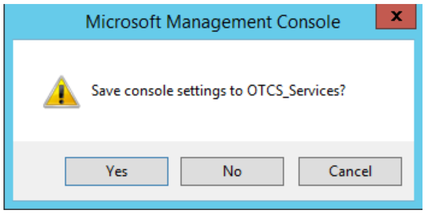
Figure 45


OTCS_Services - [Console Root\Security Configuration and Analysis]
File
Action
View
Favorites
Window
Help
New Ctrl+N
Open... Ctrl+O
Save Ctrl+S
Save As...
Add/Remove Snap-in... Ctrl+M
Options...
1 C:\Users\...\OTCS_Services
2 C:\Windows\system32\services
3 C:\Windows\system32\secpol
4 C:\Windows\system32\wf
Exit
Description

Password and account lockout policies
Auditing, user rights and security options polici...
Event Log
Restricted Groups
System service settings
Registry security settings
File system security settings

9. Click **Yes** to save the console settings.

Figure 46



Save console settings to OTCS_Services?

The service permission updates should now be complete.

OPENTEXT™

About OpenText

OpenText is the world’s largest independent provider of Enterprise Content Management (ECM) software. The Company's solutions manage information for all types of business, compliance and industry requirements in the world's largest companies, government agencies and professional service firms. OpenText supports approximately 46,000 customers and millions of users in 114 countries and 12 languages. For more information about OpenText, visit www.opentext.com.

www.opentext.com
NORTH AMERICA +800 499 6544 • UNITED STATES +1 847 267 9330 • GERMANY +49 89 4629 0
UNITED KINGDOM +44 118 984 8000 • AUSTRALIA +61 2 9026 3400