Perceptive Content Security

Best Practices

Version: 7.3.x

Written by: Product Knowledge, R&D
Date: June 2019

Hyland

Table of Contents

Security

This document provides best practices for managing security. In this document, you will find best practices defined for system architecture and application configuration, as well as auditing.

System architecture security considerations

The following sections provide system architecture security information.

OSM

The Object Storage Manager (OSM) is a critical storage element on Perceptive Content Server that stores three types of information in separate locations, including:

- Perceptive Content documents (image, TXT, PDF, and other files)
- Sub-objects, such as bitmap stamp annotations, embedded OLE annotations, thumbnails, DataCapture data, and worksheets
- Document batches that have not yet been linked or automatically processed

The OSM can store unlimited amounts of content in its original format, for example, TIFF, PDF, or Microsoft Word. By storing every page of a document as a discrete object, the OSM enables Perceptive Content to deliver pages to users on demand. The OSM is a tree structure file system that consists of a main directory comprised of sets or branches. Each set can contain 512 folders which can each contain up to 512 subdirectories. In addition, each subdirectory can contain up to 512 documents. This means that each OSM set can contain 134,217,728 documents or pieces of content. As your storage needs increase, you can set Perceptive Content to add additional OSM sets automatically.

You can configure the OSM to store objects across any number of file systems on a variety of platforms and architectural designs. This efficient, hybrid storage model ensures the Perceptive Content database maintains steady performance even as usage and database size grows.

Configure OSM

The following recommendations are steps you can perform while configuring the OSM.

- Limit OSM Windows NTFS permissions to a single Windows service account with Modify permission only.
- Consider OSM drawer redirections ensuring documents from different drawers are not in the same OSM and facilitating departmental chargeback for data storage.
- Consider other external OSM plugin solutions when adding OSM storage sets and OSM storage trees.

LDAP

Perceptive Software recommends using LDAP authentication in Perceptive Content for authenticating users. Using LDAP authentication, Perceptive Content authenticates to an LDAP server using the LDAP Simple Bind method. The Perceptive Content Server attempts a "bind" to the LDAP server using the credentials provided by the user. In addition to simple bind, Perceptive Content also supports LDAP authentication using simple bind over SSL (Secure Sockets Layer). SSL is a protocol used for transmitting documents through the Web; by default SSL connections start with https: instead of http:. Also, you can use multiple LDAP servers to authenticate against.

Encryption

WebNow transmits all data between the client's web browser and the web application server as binary data; there is no transmission of plain text. Whether the integration with WebNow is through a standard URL link or a web POST, any potentially sensitive information is hidden and will not display on the client's web browser. Thus, potentially sensitive information is always protected.

For additional security measures, an optional encryption feature can be turned on to encrypt data between the web application server and the Perceptive Content Server. Additionally, SSL encryption can be employed on the web application server to provide greater encryption between the application server and the client's web browser. WebNow also uses the Perceptive Content Client software authentication model. Therefore, security attributes are inherited when a user logs in.

Note Enabling encryption accrues approximately 10% network overhead.

Client validation

Use client validation to ensure that the Windows user account is the same account used to log into Perceptive Content.

Note Enabling client validation can cause issues when the Perceptive Content administrator troubleshoots other users' workstations.

Set up WebNow automatic Windows domain authentication

This functionality is only available when using Windows Domain authentication; it is not supported with LDAP. With automatic domain authentication enabled, you can start WebNow, while logged in on a Windows machine to an NT domain, and completely bypass the login page. If you are on a platform other than Windows or the Perceptive Content Server cannot log you in automatically, the login page appears. At this point, you should be able to log in manually.

If you provide no user name and password on the URL, and automatic domain authentication is enabled, WebNow automatically attempts to log you in. If it cannot log in, WebNow displays the login page. If you enter a user name and password on the URL, WebNow bypasses the automatic domain authentication and logs in with the information from the URL.

1. Using Windows Explorer, navigate to the [drive:]\inserver\etc folder, and then open **inow.ini**.
2. Under the **[Logon Control]** parameter, scroll to the following section and change the **client.validation** setting from FALSE to TRUE and then type the `nt.domain.list`**.**

```
; If set to true, ImageNow will allow the ImageNow client to logon with
; the User ID provided in the ImageNow logon dialog, as long as the user
; is logged into a valid Windows NT domain on the client PC with a NT
; domain account that is equal to the ImageNow user ID. Otherwise,
; ImageNow validates user and password requests via the ImageNow Server.

client.validation=TRUE

; The valid NT Domain list of which the ImageNow
; User ID must already be logged into on the requesting PC.

nt.domain.list=<<list_goes_here>>
```

3. Save and close the **inow.ini** file.
4. Restart Perceptive Content Server.

5. Complete the following steps to set domain authentication parameters in the web configuration file.
    1. Using **Windows Explorer**, navigate to the [drive:][path]\WebNow6\WEB-INF folder, and then open the **WebNow.settings** file with a text editor.
    2. Under Application server settings, change the domain-authentication setting to true.
    3. Save and close the **WebNow.settings** file.

Application configuration security considerations

The following sections provide application configuration security considerations.

Perceptive Manager and Department Manager roles

The following tables list the security rules for the Perceptive Manager and Department Manager roles.

Perceptive Manager
There can be more than one Perceptive Manager.
A Perceptive Manager cannot assign his or her own privileges.
A Perceptive Manager must be demoted before he or she can be removed from the system.
Only a Perceptive Manager can promote another user to Perceptive Manager.
Only a Perceptive Manager can import a migration package.
Only a Perceptive Manager can create a department.
A user can be a Perceptive Manager and a Department Manager simultaneously.
Only a Perceptive Manager can create users in the system.
A Perceptive Manager does not have access to Department content or configurations unless explicitly granted by a Department Manager.
Only a Perceptive Manager can promote a user to the Department Manager role.
A Perceptive Manager cannot promote himself or herself to Department Manager.

Department Manager
A Department Manager cannot create a department.
A Department Manager is the only user who can share objects in his or her department with other departments.
A Department Manager is the only user who can move items between departments on the same system.
A user can be a Department Manager for any number of departments.
One department can have multiple Department Managers.

Configure Perceptive Manager and Department Manager roles

Perceptive Software recommends the following when configuring the Perceptive Manager and Department Manager roles.

- Set up all manager users with both a manager account and a non-manager user account in the system to encourage role separation in your organization.

Views

In Perceptive Content, a view is a mechanism that displays a set of documents or folders that are selected and displayed according to the view definition that you create for your users. You can give a user access to one or more views, such that the user's overall access consists of all the documents and folders made available by the views.

When you install Perceptive Content, two default views are already in place, All documents and All folders, allowing users to have access to all documents and folders in Perceptive Content. Perceptive Software recommends that you disable these views and create individual views with assigned users.

Users

Remove the All Users group from the All Documents and the All Folders view. Create custom document and folder views for each business area.

Privileges

The Manage Process privilege will not grant access to workflow queues in that workflow process. A user who has the Manage Process privilege must still be specifically granted access to each queue within that process they need to see.