Aleph and PDS Security Best Practices

- **Product:** Aleph
- **Product Version:** 22, 23, 24
- **Relevant for Installation Type:** Multi-Tenant Direct, Dedicated-Direct, Local, TotalCare

Description

We care about your security and would like to share some best practices to keep your sensitive data secure.

Resolution

Install Aleph Service Pack and Third Party Tools

We highly recommend to always apply the latest Aleph Service Pack and Third Party Tools as well as the Operating System and Oracle Patches to close potential security gaps,.

See the latest Release Notes for Aleph Service Packs here

Release Notes - Ex Libris Knowledge Center (exlibrisgroup.com)

Are you using the Aleph Web OPAC?

Introduce XSS-Validation

/exlibris/aleph/u23_1/alephe/tab/tab100 set XSS-VALIDATION to 'Y':

XSS-VALIDATION=Y

See article

Security scans on Aleph 23 server complain about XSS Validation - Ex Libris Knowledge Center (exlibrisgroup.com)

Avoid uncertified relocate

With the default Apache configuration it is possible to relocate to a different page using option /goto.
How to avoid this situation see instructions in article Web OPAC /goto uncertified relocate - Ex Libris Knowledge Center (exlibrisgroup.com)

Are you Using the Patron Directory Service (PDS) in Aleph?

Check parameter PDS-AWARE in $alephe_tab/tab100

If `PDS-AWARE =Y`

See also article

PDS: Page is vulnerable to OS command injection attacks - Ex Libris Knowledge Center (exlibrisgroup.com)

Secure PDS

Follow the instructions of sections

- X-Server Security Patch
- Securing the PDS_HANDLE Cookie

documented in the Patron Directory Services Guide (https://knowledge.exlibrisgroup.com/@api/deki/files/26589/Patron_Directory_Services_Guide.pdf?revision=6)

No longer using Aleph Web OPAC / PDS for Aleph

Deactivate PDS on Aleph server

set the relevant line in $alephe_tab/tab100 to PDS-AWARE=N

Turn off the Web OPAC

a. Block the Web OPAC (through firewall) *or* **add a line to the file $alephe_tab/server_ip_allowed**

```
W D *.*.*.*
```

Explanation from table header

```
! COL   1.   1; ALPHA{W,P,N}, UPPER; ;
!               Server type;
!               Server type:
!               W = WWW web server
!               X = X-Server (part of WWW web server services)
!               P = PC server
!               N = NCIP server;
! COL   2.   1; ALPHA{A,D}, UPPER; ;
!               Access permission;
```

```
!               Access permission:
!               A - Allowed
!               D - Denied;
```

Note: if you are using a discovery system, add the IP address to file $alephe_tab/server_ip_allowed as follows. In this case please ignore the next sections (b+c).

Example

```
W A 123.123.456.456
```

b. Stop the WWW Server

In case you are using the X-Server for communication with your discovery system (e.g. Primo) the WWW server should not be stopped.

- Connect to your Aleph server (using ssh)
- `dlib xxx01`
- **`Util W / 2. Stop Servers / 2.  WWW Server to stop`** `the WWW Server`

c. Deactivate the automatic startup of the WWW Server

Remove the following section from $alephe_root/aleph_startup configuration

```
    if  (! $?WWW_START_HOST) then
            echo "starting www_server...."
            csh -f $aleph_proc/www_server $l_www_server_port $l_httpd_port $l_n_of_servers
>& /dev/null &
            echo " "
        else
            foreach thishost ($WWW_START_HOST)
                if  ($thishost == $THIS_HOST) then
                    echo "starting www_server...."
                    csh -f $aleph_proc/www_server $l_www_server_port $l_httpd_port
$l_n_of_servers >& /dev/null &
                    echo " "
                endif
            end
        endif
```

If you are using Primo and the Aleph Web OPAC

consider turning off the Aleph Web OPAC and PDS as above

If SSO for Aleph and Primo is required: introduce the above measures listed under **Secure PDS**

If you are using Primo with PDS

Consider turning off PDS and moving to Primo User Authentication (Aleph 22 and up)

see

Primo User Authentication - Ex Libris Knowledge Center (exlibrisgroup.com)

Primo Authentication Manager – With this method, Primo interacts directly with the institution's authentication server and supports authentication using SAML, CAS, LDAP, Aleph, Alma, and social login via Alma. **Customers who want to switch from PDS to this method should contact to Ex Libris Support.** For more information, see The Primo Authentication Manager.

- **Article last edited:** 07-March-2024