



**US Army Corps
of Engineers®**
Engineer Research and
Development Center



ERDC Technology Transfer and Infusion/Knowledge Management

Mindbreeze InSpire Search Appliance Implementation and Lessons Learned

Byron M. Garton, Jonathan S. Broderick,
and Michael A. Clement

September 2020

The U.S. Army Engineer Research and Development Center (ERDC) solves the nation's toughest engineering and environmental challenges. ERDC develops innovative solutions in civil and military engineering, geospatial sciences, water resources, and environmental sciences for the Army, the Department of Defense, civilian agencies, and our nation's public good. Find out more at www.erdclibrary.on.worldcat.org/discovery.

To search for other technical reports published by ERDC, visit the ERDC online library at www.erdclibrary.on.worldcat.org/discovery.

Mindbreeze InSpire Search Appliance Implementation and Lessons Learned

Byron M. Garton, Jonathan S. Broderick, and Michael A. Clement

*Information Technology Laboratory
U.S. Army Engineer Research and Development Center
3909 Halls Ferry Road
Vicksburg, MS 39180-6199*

Final report

Approved for public release; distribution is unlimited.

Prepared for ERDC Office of Research and Technology Transfer (ORTT)
3909 Halls Ferry Road
Vicksburg, MS 39180-6199

Under ERDC Office of Research and Technology Transfer (ORTT), WIC 19F1H5

Abstract

The U.S. Army Engineer Research and Development Center (ERDC) Knowledge Management relies on enterprise search technology to index and search ERDC's accumulation of knowledge stored on various web connected systems. In 2016, Google announced the discontinuation of their search product, the Google Search Appliance (GSA), at the end of March 2019. After conducting extensive market research and identifying a suitable replacement that met all ERDC requirements, a competing product called Mindbreeze InSpire was chosen. This product provides a simple-to-use interface that facilitates quick location and retrieval of ERDC knowledge located on ERDC's internal and extranet websites, and is designed for simple and intuitive installation and configuration.

This document investigates and details the acquisition, installation, and configuration of the Mindbreeze InSpire enterprise search appliance, and the lessons learned throughout the entire implementation process.

DISCLAIMER: The contents of this report are not to be used for advertising, publication, or promotional purposes. Citation of trade names does not constitute an official endorsement or approval of the use of such commercial products. All product names and trademarks cited are the property of their respective owners. The findings of this report are not to be construed as an official Department of the Army position unless so designated by other authorized documents.

DESTROY THIS REPORT WHEN NO LONGER NEEDED. DO NOT RETURN IT TO THE ORIGINATOR.

Contents

Abstract.....	ii
Figures	iv
Preface	v
1 Introduction.....	1
Purpose.....	1
Scope	1
Overview	2
2 Acquisition.....	3
3 Installation	4
iDRAC setup.....	4
NIC setup	9
4 Configuration	14
Management center console.....	14
<i>Management center console login.....</i>	<i>14</i>
<i>GSA configuration file migration</i>	<i>15</i>
<i>Management center setup section functions.....</i>	<i>18</i>
<i>Management center configuration section functions.....</i>	<i>21</i>
Customizing the client service.....	31
5 Maintenance.....	34
Software updates.....	34
Indexes.....	35
Certificate and license	36
6 Backup Strategies.....	37
7 Lessons Learned.....	38
Acquisition	38
Installation	38
Configuration	39
Acronyms and Abbreviations	41
Report Documentation Page	

Figures

Figure 1. Server front LCD panel.....	4
Figure 2. iDRAC login screen.	5
Figure 3. iDRAC dashboard screen.....	6
Figure 4. Change the default password screen.	7
Figure 5. iDRAC network settings screen.....	8
Figure 6. MAC addresses for iDRAC and NIC.....	9
Figure 7. iDRAC virtual console.	10
Figure 8. Virtual console login.....	10
Figure 9. NetworkManager TUI screen.....	11
Figure 10. Select NIC screen.....	11
Figure 11. Edit connection screen.....	12
Figure 12. NIC backup configuration.....	13
Figure 13. Management center login screen.	14
Figure 14. Management center home screen.....	15
Figure 15. File manager screen.....	17
Figure 16. Management center InSpire container restart.	18
Figure 17. Node list screen.....	19
Figure 18. Node editor screen.	19
Figure 19. Node properties screen.....	20
Figure 20. SSL certificate upload screen.....	21
Figure 21. Management center configuration screen.....	22
Figure 22. Indices configuration screen.	23
Figure 23. Index data sources.	24
Figure 24. Client services configuration screen.....	26
Figure 25. Custom client service configuration.....	27
Figure 26. License management screen.....	28
Figure 27. Certificates management screen.	29
Figure 28. SAML configuration.	30
Figure 29. Copy file using file manager.....	31
Figure 30. ERDC's customized client service.	33
Figure 31. Upload Mindbreeze update.....	34
Figure 32. Software update success.....	35

Preface

This research was conducted for the ERDC Office of Research and Technology Transfer (ORTT) utilizing Future Innovation Funds (FIF) for, “*ERDC Technology Transfer and Infusion/Knowledge Management*,” by the ERDC Information Technology Laboratory (ITL). The technical monitor was Ms. Antisa C. Webb.

The work was performed by the Scientific Software Branch (SSB) of the Computational Science and Engineering Division (CSED), U.S. Army Engineer Research and Development Center – Information Technology Laboratory (ERDC-ITL). At the time of publication, Mr. Timothy W. Dunaway was Chief, SSB; and Dr. Jerrell R. Ballard, Jr. was Chief, CSED. The Deputy Director of ITL was Ms. Patti S. Duett and the Director was Dr. David A. Horner.

COL Teresa A. Schlosser was the Commander of ERDC, and Dr. David W. Pittman was the Director.

1 Introduction

Purpose

The U.S. Army Engineer Research and Development Center (ERDC) has embarked on several knowledge management initiatives over the years in an effort to make the accumulation of knowledge easier to catalog, locate, and share. These initiatives have been focused on a combination of technologies including enterprise search. Until FY 2019, ERDC had relied upon Google's enterprise search appliance product (GSA) to index content and provide a simple and intuitive search interface to users. Unfortunately, Google announced discontinuation of its search appliance in February of 2016. End of life was scheduled for March 2019, and no new licenses were issued after 2016.

Scope

After being notified of the GSA discontinuation by Google, research was begun at ERDC-ITL to identify a suitable replacement search appliance. First, a set of baseline requirements were defined. Candidate systems must meet certain requirements in the areas of functionality, ease of installation, long-term viability, initial and recurring costs, and maintenance. Baseline functionality of a GSA replacement system must account for the following capabilities:

1. Hardware must meet or exceed current GSA hardware capabilities.
2. Installation of the replacement system must be easily achieved by existing ERDC personnel or contracted labor from the product vendor.
3. The ability to index internal and extranet content on ERDC servers within the Research and Development Environment (RDE) network.
4. Support existing RDE authentication methods for knowledge consumers and provide a method for authentication while indexing content on servers that require authentication prior to access.
5. Provide a customizable user interface, allow searches to be made on the indexed data, and output results in an easy to use and understandable format.
6. No limit on the size or number of indexes that can be made or provide simple methods to increase the number of allowable indexes in order to scale and satisfy long-term viability requirements.

7. Software must be customizable in order to meet unforeseen future requirements through the use of open-source software or timely customization from the product vendor.
8. The ability to acquire security certifications for installation on RDE network prior to GSA end of life.
9. Provide responsive and timely technical support when problems arise.

Overview

Extensive online research was conducted to identify private industry companies and products that could potentially meet the baseline requirements identified. Each company was contacted and asked to provide information related to these requirements. After collecting and analyzing the data supplied and comparing to the requirements, the Mindbreeze InSpire was selected based on its ability to satisfy all of ERDC's search requirements.

2 Acquisition

Mindbreeze GmbH is a privately held company based in Linz, Austria with a U.S. based distributor, Onix Networking Corp. based in Lakewood, OH. Onix holds current government purchase contracts on various purchase vehicles.

Contact was made with Onix to request a quote for a quantity of two Mindbreeze InSpire model M102 enterprise search appliances with licenses for 500,000 indexes each. The quote received from Onix totaled \$67,500. The Information Technology Laboratory (ITL) Management Integration Office (MIO) and contracting specialists took over at that point to complete the transaction through the Army Computer Hardware Enterprise Software and Solutions (CHESS) supplies and equipment contract purchase process.

The contract was awarded in September 2018 for Onix to ship the two appliances for the agreed upon quote amount. Logistics at ERDC received the shipment in October 2018, and the equipment was delivered to and received at ITL in December 2018. A license file was also supplied to ITL by Onix support via email attachment following the completed purchase.

3 Installation

The installation process includes tasks that require physical access to the appliances in order to be completed. Mindbreeze InSpire search appliances are based on Dell PowerEdge rack mounted server hardware. The units are each 2RU in size, which means they occupy two units of vertical space in a server rack. Upon receiving the appliances, contact was made with RDE support to arrange for physical installation on the RDE network by appropriate personnel.

Once the appliances were physically installed in an RDE server rack, network cables were routed through the data center and connected. There are two sets of network ports on the Mindbreeze InSpire: two Integrated Dell Remote Access Controller (iDRAC) ports, and 4 Network Interface Card (NIC) ports. The NIC is where all search traffic (indexing and querying) will enter and exit the appliance. It is considered the “public” interface, where the iDRAC is considered the “administrative” interface. A total of 3 network cables must be run from the InSpire to a nearby RDE router or switch: one for iDRAC #1, and two for NIC #1 and 2.

iDRAC setup

Being an interface to the configuration console of the server, the iDRAC port allows configuration of the IP information for the appliance. Physical access to the server is required along with a network patch cable connected to the NIC on a laptop computer. The iDRAC IP address must be changed via the LCD panel on the front of the appliance to allow access to the configuration interface (Figure 1).

Figure 1. Server front LCD panel.

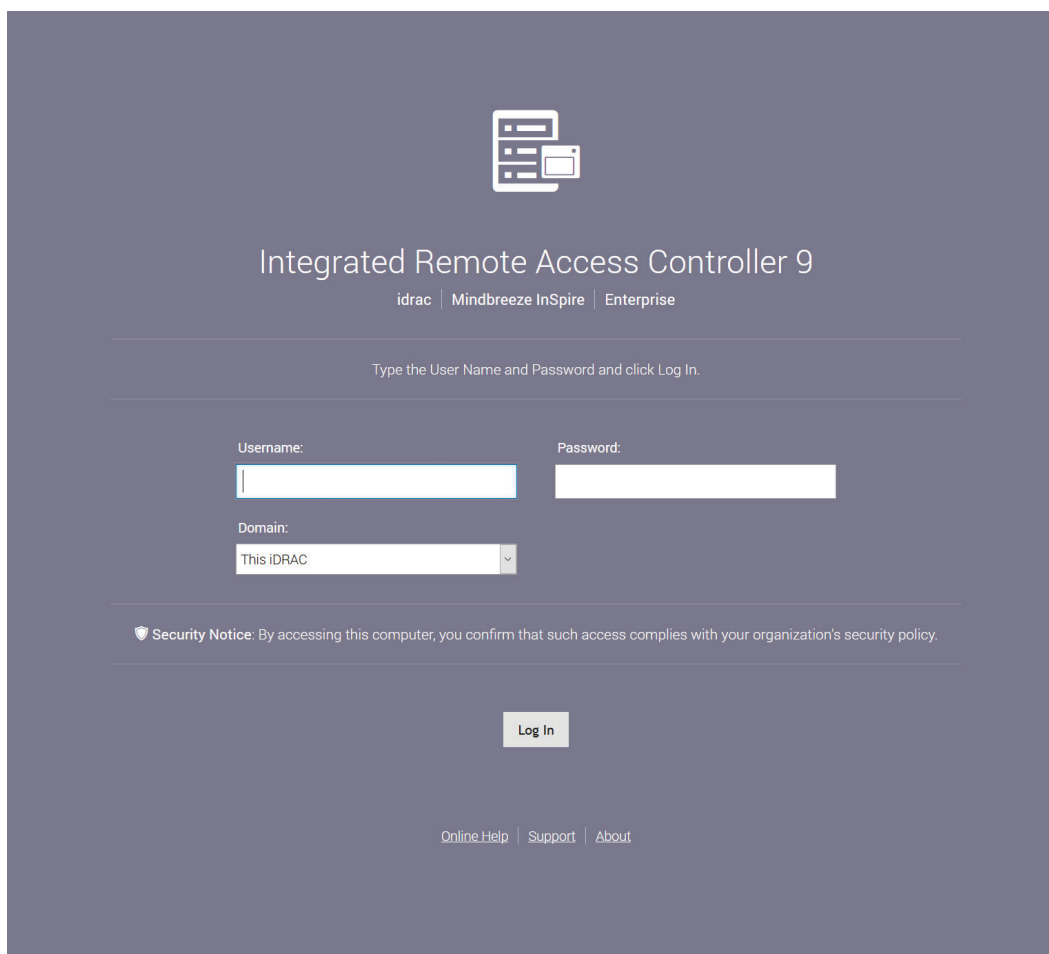


To set the IP address using the front LCD panel, navigate from the Home screen to the Setup screen, then select the Static IP tab. From this screen, use the arrow keys to first select IP and set each octet to a standard private IP address of 192.168.1.1. Continue by selecting Sub, and enter the subnet mask of 255.255.255.0. Finally, select Gtw and enter the same IP address entered previously, 192.168.1.1 as the default gateway address.

An actual working default gateway is not necessary at this point since the iDRAC will not be accessing the internet, but is required to be set up.

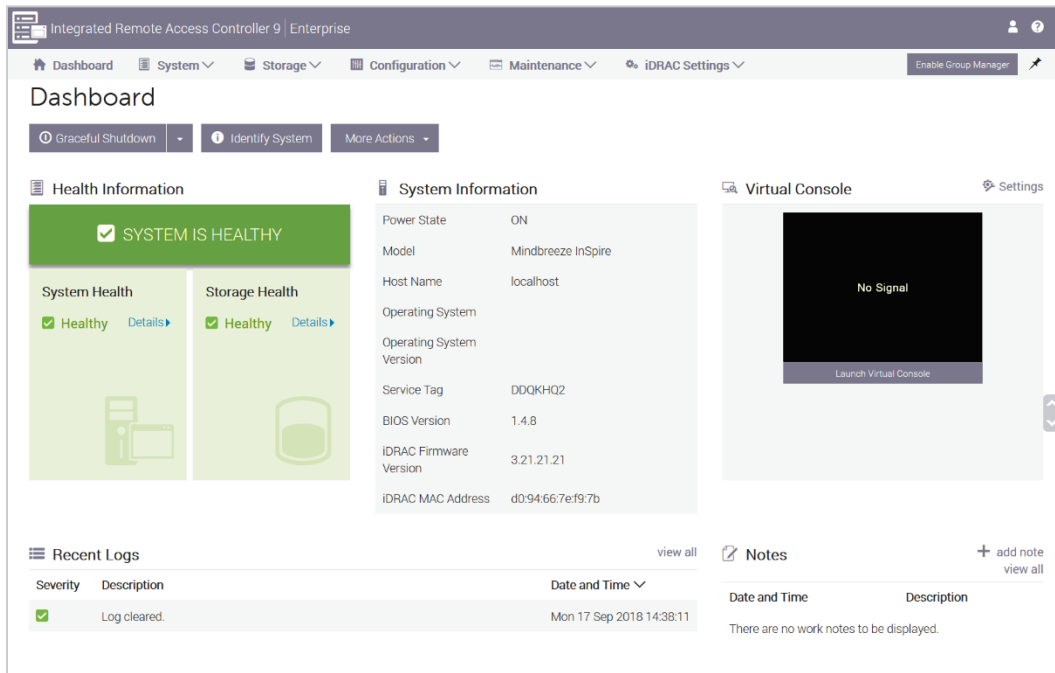
Next, configure the laptop network interface to 192.168.1.2 and subnet mask to 255.255.255.0 by following the standard procedure for the particular operating system being used. Use an internet browser of choice to connect to the iDRAC IP address 192.168.1.1, which will bring up the login screen seen in Figure 2.

Figure 2. iDRAC login screen.

The image shows the login interface for the Integrated Remote Access Controller 9. At the top center is a logo consisting of a server rack icon and a monitor icon. Below the logo, the text "Integrated Remote Access Controller 9" is displayed in a large, white font. Underneath this, in a smaller font, are the words "idrac | Mindbreeze InSpire | Enterprise". A horizontal line separates the header from the login instructions, which read "Type the User Name and Password and click Log In." Below this, there are three input fields: "Username:" with a text box, "Password:" with a text box, and "Domain:" with a dropdown menu currently showing "This iDRAC". A "Log In" button is positioned below these fields. At the bottom of the form, there is a "Security Notice" section with a shield icon and the text: "Security Notice: By accessing this computer, you confirm that such access complies with your organization's security policy." At the very bottom of the page, there are links for "Online Help", "Support", and "About".

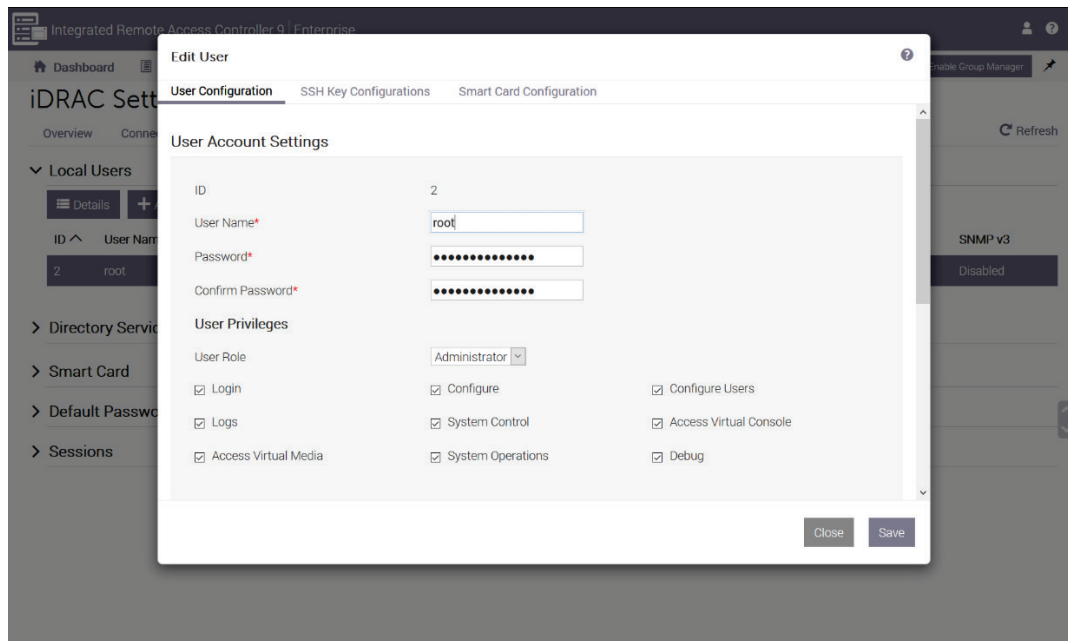
The default username and password combination is defined in the Mindbreeze documentation or found on their website support pages. The default password can and should be changed after logging in. Figure 3 shows the dashboard screen that is shown after logging in successfully.

Figure 3. iDRAC dashboard screen.



There are many settings that can be configured from this screen, but only two are of interest to initial setup: changing the default password and IP address settings. Both are located on the iDRAC Settings tab at the top of the dashboard screen. Inside iDRAC Settings, click the Users tab to change the default password. Only one user is defined, so click the Edit button to open the password editor. Use the Save button to change the password after entering twice as shown in Figure 4.

Figure 4. Change the default password screen.



Next, change the IP address settings by going back to the iDRAC Settings screen and click the Connectivity tab. On that screen, click the Arrow to the left of Network to expand that section. Next, find IPv4 Settings and click the Arrow to the left. This is where the IP settings for the iDRAC connection are changed. RDE must make the necessary configurations on their routing equipment and provide the IP information to use in these boxes. In addition to IP address information, RDE will (upon request) provide Domain Name Service (DNS) that links the IP address to a domain name. For this project, the URL provided by RDE was <https://search.erdcdren.mil>.

Figure 5. iDRAC network settings screen.

Integrated Remote Access Controller 9 | Enterprise

Dashboard System Storage Configuration Maintenance iDRAC Settings Enable Group Manager

iDRAC Settings

Overview **Connectivity** Services Users Settings Refresh

Network

- Network Settings
- Common Settings
- Auto Config

IPv4 Settings

Enabled IPv4	Enabled
DHCP	Disabled
Static IP Address*	10.200.150.190
Static Gateway*	10.200.150.254
Static Subnet Mask*	255.255.255.0
Use DHCP to Obtain DNS Server Addresses	Disabled
Static Preferred DNS Server	0.0.0.0
Static Alternate DNS Server	0.0.0.0

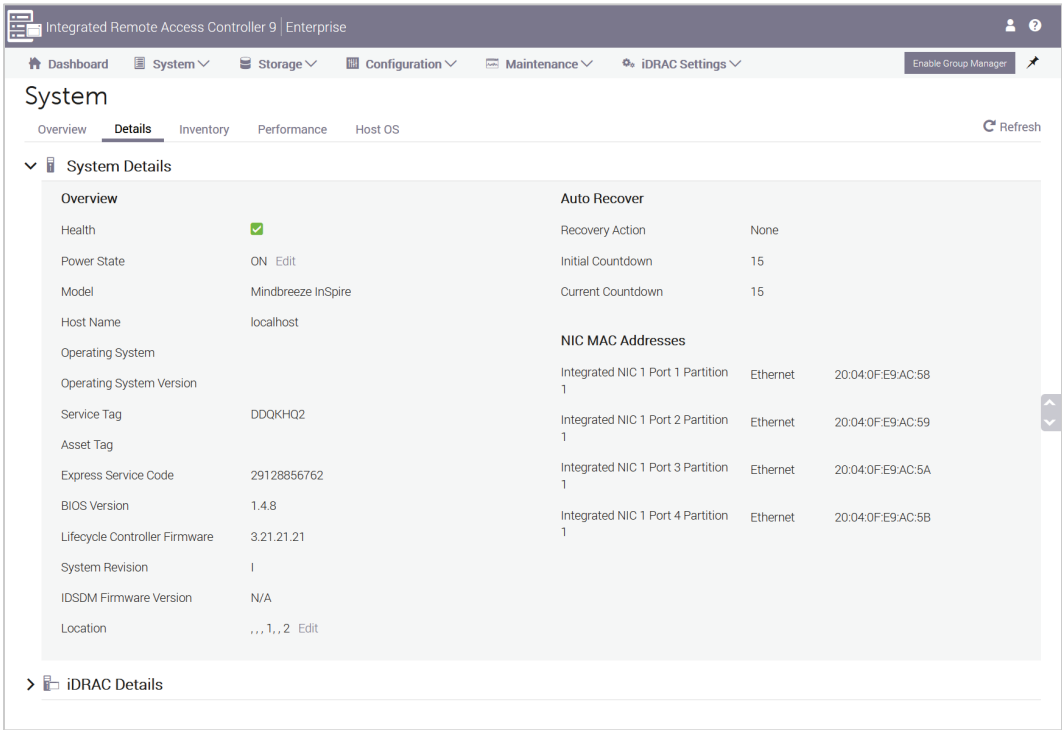
Apply Discard

IPv6 Settings

IPMI Settings

RDE will need to know the Media Access Control (MAC) address information for the network connections beforehand. MAC addresses for the iDRAC and NIC are found on the System Details screen by clicking the System tab at the top, then clicking the Details tab as shown in Figure 6. Use the Arrow to expand System Details for the NIC addresses and iDRAC Details for the iDRAC address.

Figure 6. MAC addresses for iDRAC and NIC.



NIC setup

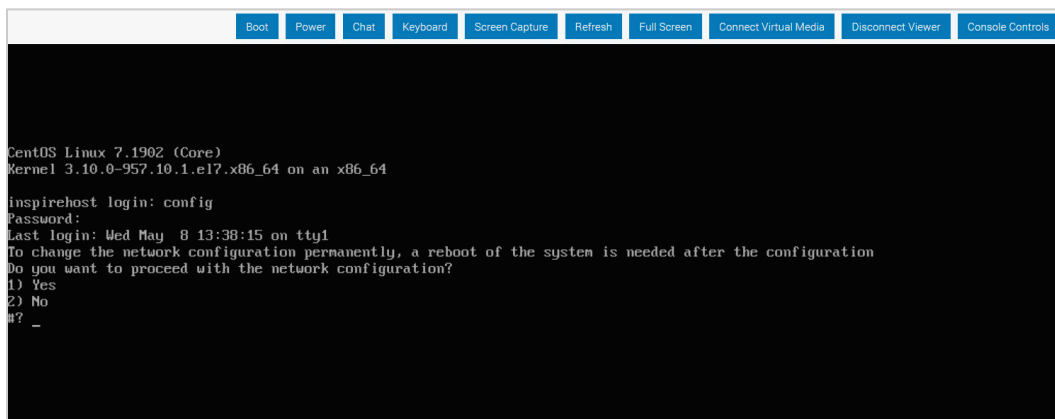
Once the iDRAC IP information is configured, the IP information for the NIC ports must be configured. Configuring the NIC is done from the iDRAC Virtual Console. On the iDRAC dashboard, click the Virtual Console to launch in a new window. The browser may block it as a popup, so an exception may need to be added. The virtual console window can be seen in Figure 7.

Figure 7. iDRAC virtual console.



Click the Power button to power on the virtual console and when prompted, choose Power Cycle System (cold boot). Once the console has booted up, log in with the default username and password combination found in the Mindbreeze documentation or on their support website (Figure 8).

Figure 8. Virtual console login.



When prompted to change network configuration, enter 1 and press Enter to continue. Next, select Edit a Connection from the NetworkManager TUI screen, then select bond0 as shown in Figures 9 - 11.

Figure 9. NetworkManager TUI screen.

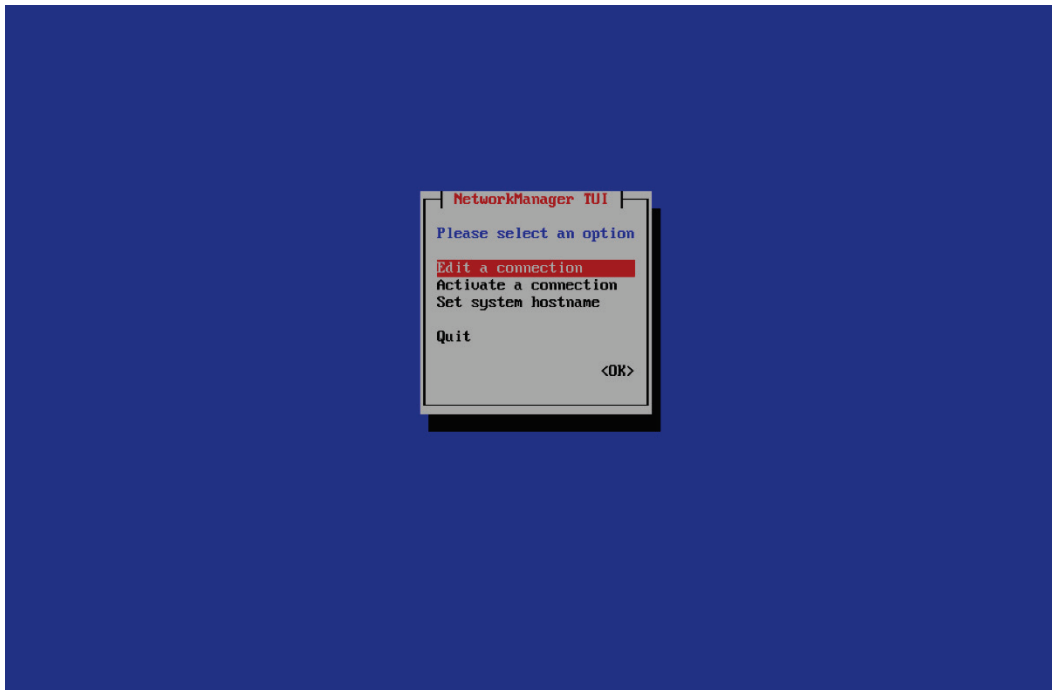


Figure 10. Select NIC screen.

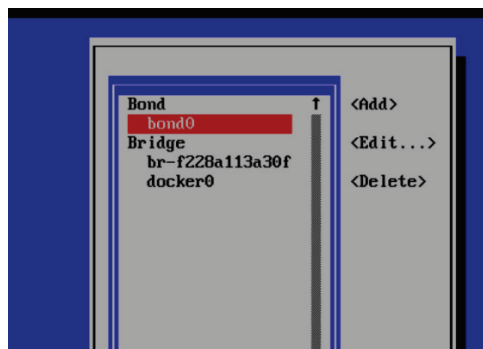


Figure 11. Edit connection screen.

Edit Connection

Profile name: bond0
Device: bond0

BOND Slaves <Hide>

eno2
eno1
eno3
eno4

<Add>
<Edit...>
<Delete>

Mode: <Active Backup>
Primary: eno1
Link monitoring: <MII (recommended)>
Monitoring frequency: 100 ms
Link up delay: 0 ms
Link down delay: 0 ms

IPv4 CONFIGURATION <Manual> <Hide>

Addresses: <Add...>
Gateway: <Add...>
DNS servers: <Add...>
Search domains: <Add...>

Routing (No custom routes) <Edit...>
☐ Never use this network for default route
☐ Ignore automatically obtained routes
☐ Require IPv4 addressing for this connection

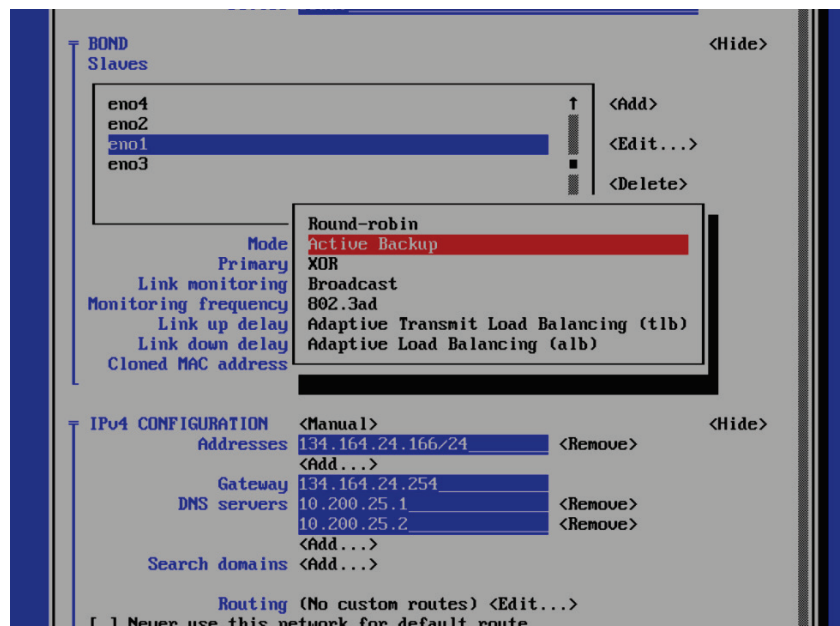
IPv6 CONFIGURATION <Automatic> <Show>

☒ Automatically connect
☒ Available to all users

<Cancel> <OK>

Each port on the NIC corresponds with an item in the Slaves section of this screen. In the IPv4 section, locate <Add...> and press Enter to add IP address information. With the information received from RDE, complete the Gateway and DNS Servers sections the same way. Only one NIC port is required to be configured, but setting up a backup method is highly recommended. Locate Mode and press Enter, then choose <Active Backup>. Select eno1 as Primary to complete the backup method configuration (Figure 12).

Figure 12. NIC backup configuration.



After completing IP configuration, navigate to the bottom of the screen and choose OK. Choose Back from the next screen, then Quit from the start screen to exit. This will shut down the server and force a reboot. Installation is now complete, and configuration can begin.

4 Configuration

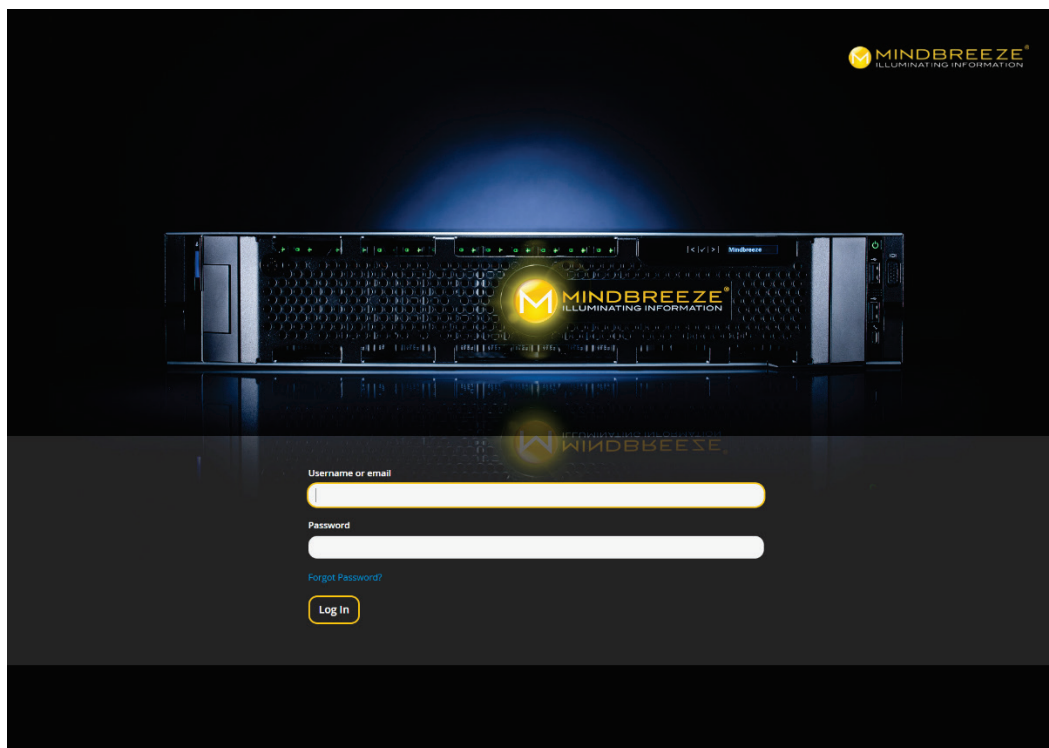
Management center console

There are a multitude of configuration changes required to make the Mindbreeze InSpire search appliance functional. Mindbreeze has attempted to make the configuration of the appliance as painless as possible by integrating a browser-based configuration management console application called Management Center that utilizes a simple and intuitive user interface.

Management center console login

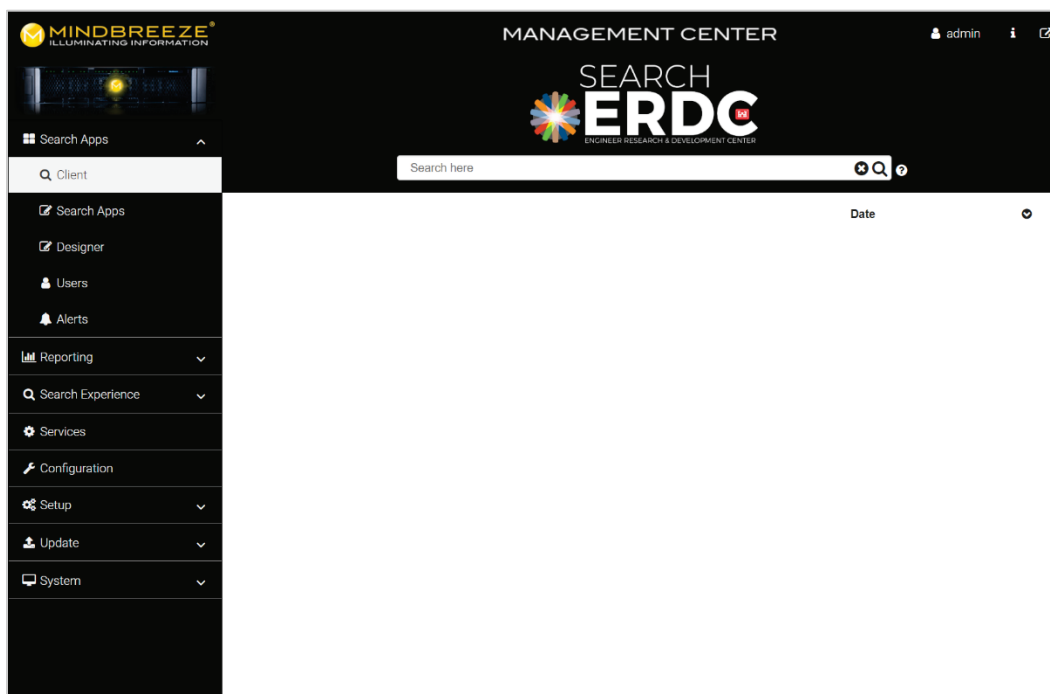
To access the configuration management console, launch a web browser of choice and enter the URL supplied by RDE. Direct the browser to use port 8443 by modifying the end of the URL in the following manner: <https://search.erdc.dren.mil:8443>. The management console login screen will appear as shown in Figure 13. Log in to the console with the default username and password combination from Mindbreeze.

Figure 13. Management center login screen.



On the home screen, there is a menu on the left side of the window that contains all available configuration functions. By default, Search Apps is opened, and the search client is opened in the right-side pane. The custom search app created for this project is shown in Figure 14.

Figure 14. Management center home screen.



The default password should be changed immediately. Click Setup in the left-side menu, then click Credentials. Next, locate the Manage section and click on Users. Click the View all users button, then the Edit button on the right side of the admin user row. Click the Credentials tab and enter a new password twice, then click the Reset Password button to complete the task.

Not all configuration items in the Management Center were required when setting up the appliance, but the items that did require configuration are detailed below.

GSA configuration file migration

Since this project involved a migration from a current production GSA to a Mindbreeze InSpire appliance, some configuration was done automatically. Mindbreeze offers a free GSA configuration migration service to customers, which involves converting the current GSA

configuration file to a Mindbreeze formatted configuration file. This conversion process accomplishes the task of migrating over the data source URLs from the GSA along with any specialized indexing rules for those sources. For example, a server that stores information to be indexed has a URL that is used to locate it on the RDE network. Additionally, that server may have some data folders that should not be indexed. The solution for this is to define an exclusion rule that prevents the indexing service from reading data in that location. These rules are written in a special text processing language called regular expressions. Mindbreeze will take the URLs and associated rules from the GSA configuration file, convert them to Mindbreeze syntax, then add them to the Mindbreeze configuration file to assist the GSA migration process.

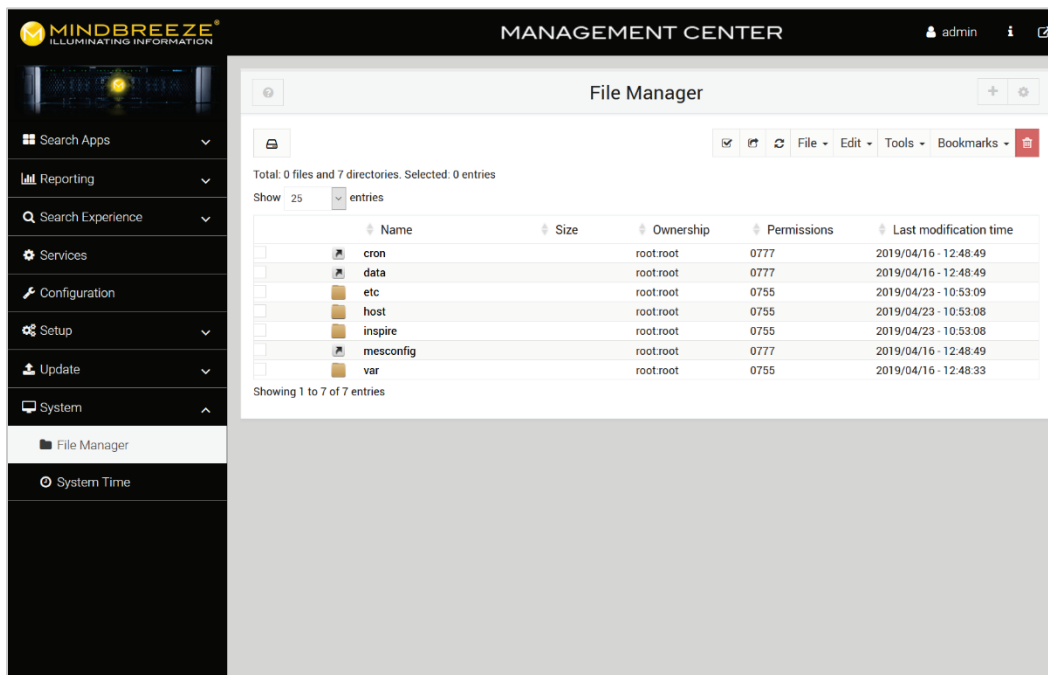
Both the GSA and Mindbreeze configuration files are written in the XML markup language. It is necessary to acquire both files before initiating the migration service with Mindbreeze. Follow the steps below to acquire a copy of the GSA configuration file.

1. Log in to the Admin Console.
2. Click **Administration > Import/Export**.
3. In the **Export Configuration** section of the page, enter a passphrase to use for import and export operations. The passphrase must be at least eight characters long.
4. Retype the passphrase.
5. Click the **Export Configuration** button.
6. Browse to a location on the local computer for the file and click **Save**.

Use the Mindbreeze management console to locate and download a copy of the Mindbreeze configuration file using the following steps and Figure 15.

1. Log in to the Management Center console.
2. Click **System > File Manager**.
3. Navigate to `> inspire/config/etc/mindbreeze/mesconfig.xml`
4. Click the `mesconfig.xml` file to download.

Figure 15. File manager screen.

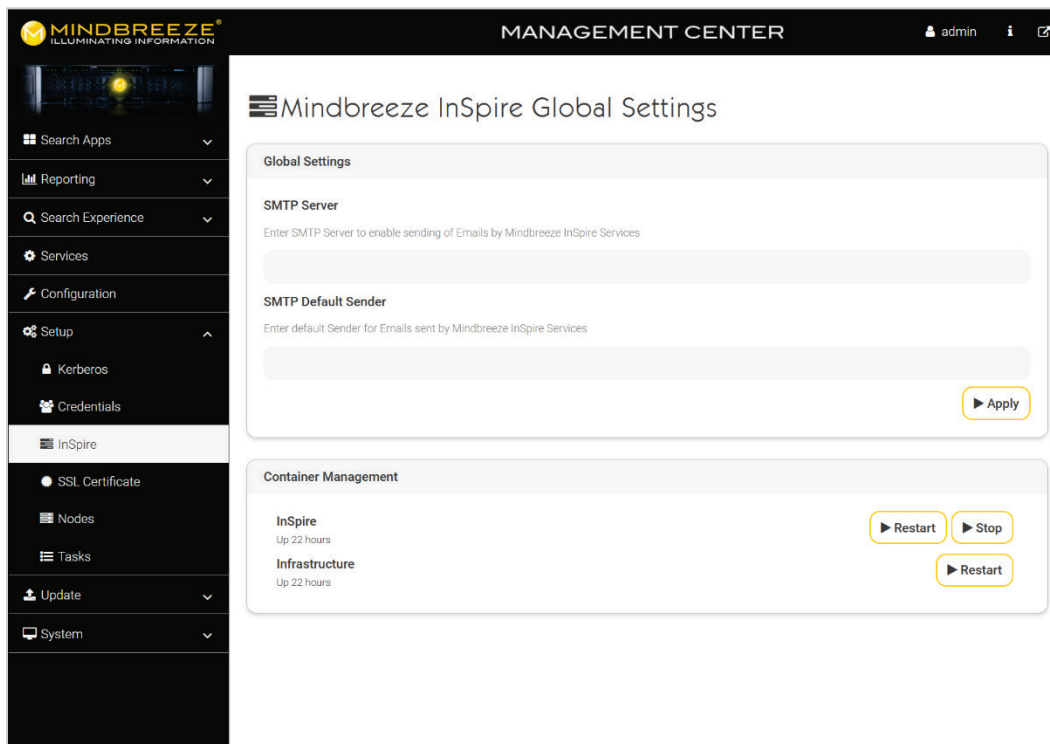


To initiate the migration process, open a new Mindbreeze support ticket at <https://tickets.mindbreeze.com> requesting a configuration file migration, then attach the two XML configuration files to the request. Turnaround for the migration service is generally 3 to 5 business days.

Once the converted `mesconfig.xml` file has been received, use the previous instructions for locating the file to return the new file to that folder location. Choose yes if prompted for confirmation to overwrite the existing file.

Finally, the InSpire container must be restarted for the changes to take effect. Use the Management Center console to initiate a restart. Click Setup in the left-side menu, click InSpire below, then in the Container Management section, click the Restart button as seen in Figure 16 to restart InSpire.

Figure 16. Management center InSpire container restart.



Management center setup section functions

The Setup section contains two key configuration items that must be done prior to any other configuration. Mindbreeze designed the InSpire appliance with the ability to create individual processes within the software called Nodes. These Nodes are designed to handle processes independently and are used to divide the work load of indexing, filtering, and serving search results to the client interface into individual containers. The purpose of this is to separate duties so they can independently be restarted or configured without upsetting each other and for load balancing across multiple appliances. For ERDC's purpose, only one node was required since all services are performed on only one appliance. Click on Nodes to add a node and edit its properties as shown in Figures 17 and 18.

Figure 17. Node list screen.

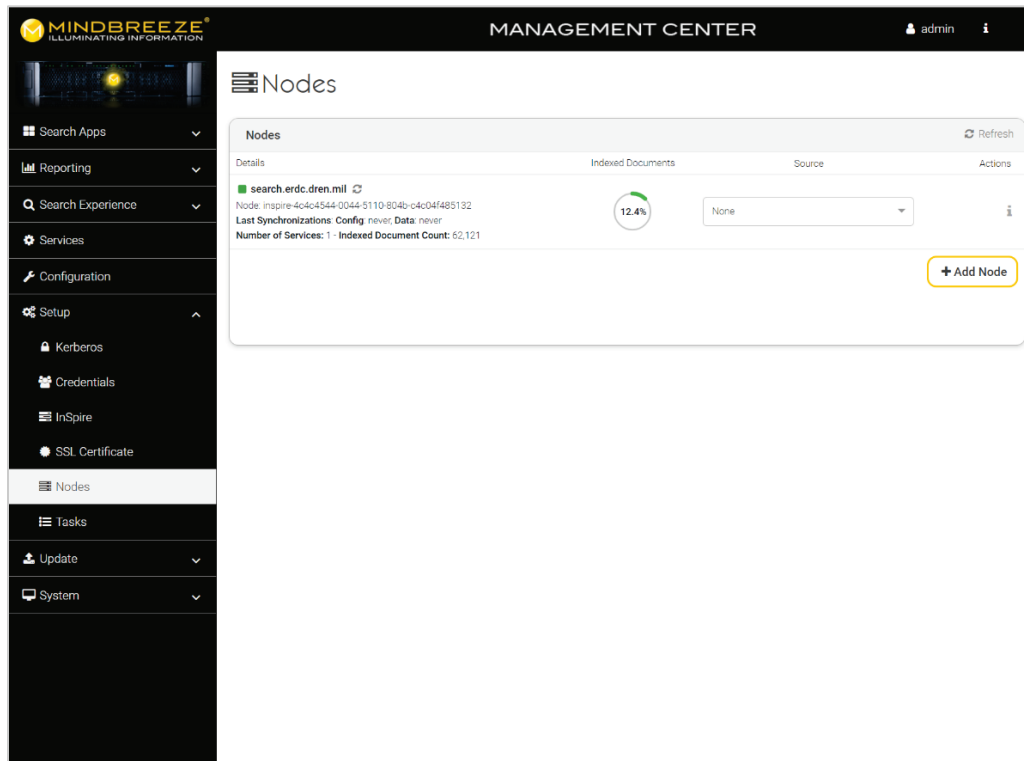
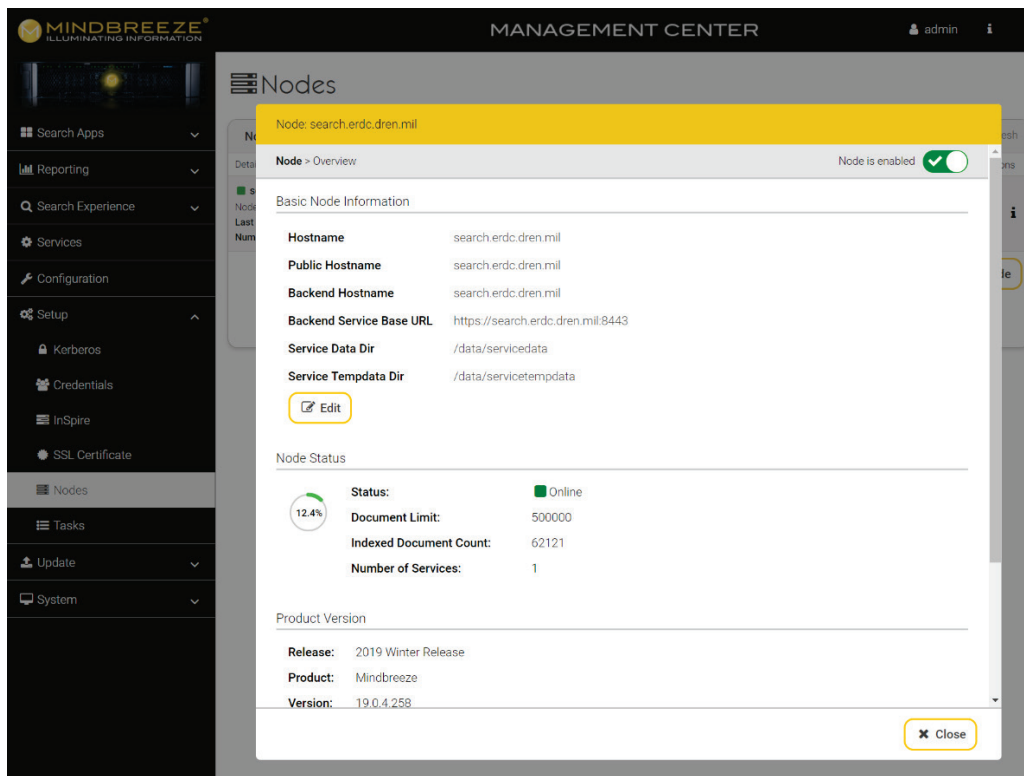


Figure 18. Node editor screen.



Click the Add Node button to create a new node and enter the server URL provided by RDE into the Hostname, Public Hostname, and Backend Hostname as shown in Figure 19, then click the Save button to create the new node.

Figure 19. Node properties screen.

The screenshot displays the 'Node properties screen' for a node named 'search.ercd.dren.mil'. The interface includes several input fields and buttons:

- Hostname:** Input field containing 'search.ercd.dren.mil' with a 'reset' button.
- Public Hostname:** Input field containing 'search.ercd.dren.mil' with a 'reset' button.
- Backend Hostname:** Input field containing 'search.ercd.dren.mil' with a 'reset' button.
- Backend Service Base URL:** Input field containing 'https://search.ercd.dren.mil:8443' with a 'reset' button.
- Service Data Dir:** Input field containing '/data/servicedata'.
- Service Tempdata Dir:** Input field containing '/data/servicetempdata'.

At the bottom right, there are two buttons: 'Abort' (with a close icon) and 'Save' (with a save icon).

Another key configuration item in the Setup section is SSL Certificate. Secure Sockets Layer (SSL) is an encryption standard for website traffic and is required on all RDE connected systems. A request must be made to RDE an SSL certificate for the appliance to be created. The certificate should be in the PKCS 12 file format (<filename>.p12). Once the certificate is provided, click SSL Certificate to upload it to the appliance. RDE does not generally require a password with their SSL certificates, but if there is a password set, enter it into the Password box as shown in Figure 20.

Figure 20. SSL certificate upload screen.

Upload Mindbreeze InSpire Certificate

Upload Certificate

Choose Certificate File

Certificate No file chosen Choose File

upload

Password

Upload File

[Download Log](#)

Management center configuration section functions

A majority of the required configuration items exist in the Configuration section. Configuring the index, filters, client service, license file, certificates, authentication, network settings, and plugins all occurs in this section. Click Configuration in the left-side menu to open the configuration section in the right-side pane as shown in Figure 21.

Figure 21. Management center configuration screen.

MINDBREEZE
ILLUMINATING INFORMATION

MANAGEMENT CENTER

Copyright (c) Mindbreeze GmbH, Linz, Austria, 2005-2019
Mindbreeze (2019 Winter Release)
Configuration

Overview Indices Filters Client Services License Certificates Authentication Network Plugins About

Services (4)

Service Name	Node	Associated Index
Client Service	search.erc.dren.mil	
Crawler Service Web	search.erc.dren.mil	Index Service /data/indices/web-test
Index Service	search.erc.dren.mil	Index Service /data/indices/web-test
Filter Service	search.erc.dren.mil	
Filter Service (Auto Mode)	search.erc.dren.mil	

Nodes (3)

OS	Node	Number of Services
inspire-4c4c544-0044-5110-804b-c4c64f485132		0
search.erc.dren.mil	inspire-4c4c544-0044-5110-804b-c4c64f485132	3
inspire-4c4c544-0044-5110-804b-c4c64f485132		500000
inspire-4c4c544-0044-5110-804b-c4c64f485132	inspire-4c4c544-0044-5110-804b-c4c64f485132	0

Category Plugins (47)

Category	Access Interface Library	Context Interface Library
Atlassian Confluence	confluence-authorization.jar (ver. 19.0.4.65)	
Atlassian Jira	atlassian-jira.jar (ver. 19.0.4.65)	atlassian-jira.jar (ver. 19.0.4.65)
AuthorizedWeb	filesystem-access.jar (ver. 19.0.4.65)	contextualization.jar (ver. 19.0.4.65)
BestBets	bestbets-datasource.jar (ver. 19.0.4.65)	bestbets-datasource.jar (ver. 19.0.4.65)
Category	filesystem-access.jar (ver. 1.0.0.0)	
DataIntegration	authorization.jar (ver. 19.0.4.65)	contextualization.jar (ver. 19.0.4.65)
EMC Documentum	authorization.jar (ver. 19.0.4.65)	contextualization.jar (ver. 19.0.4.65)

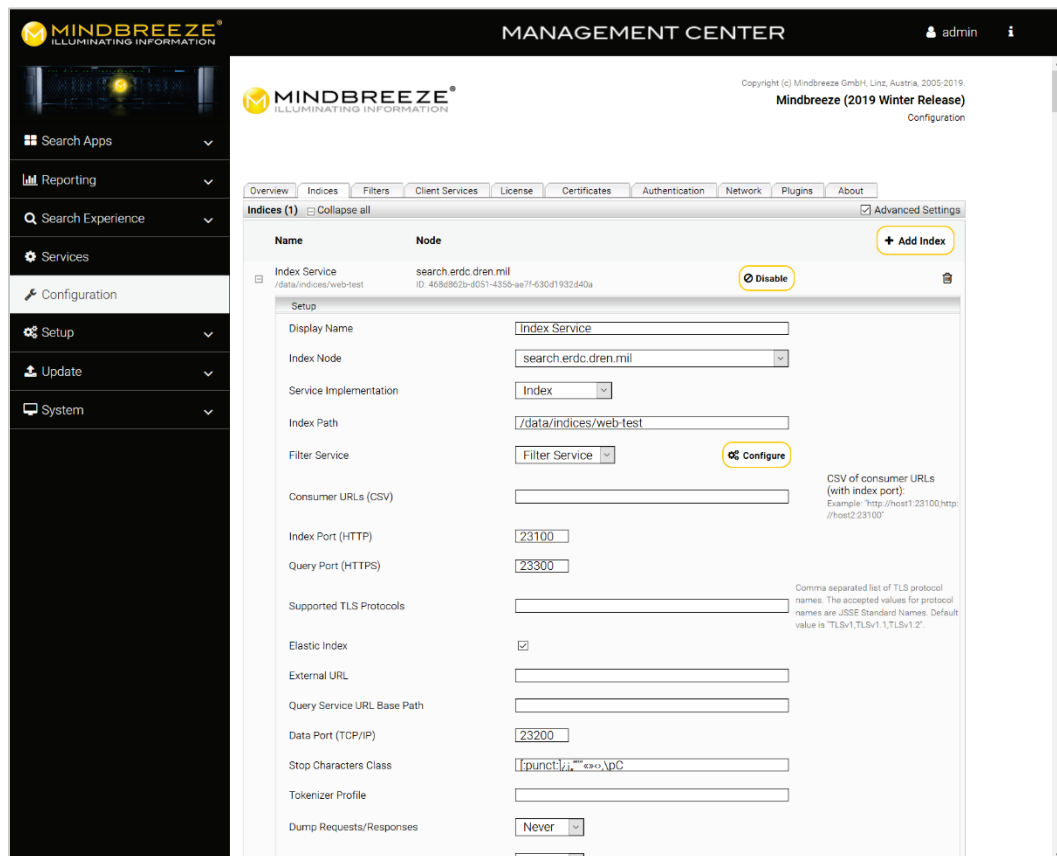
All configuration items are listed in tabs across the top. The major items of concern are Indices, Client Services, License, Certificates, and Authentication.

Indices tab

This tab is where the index service is configured. The index service reaches out to data sources and retrieves content to be indexed. Much of the index service configuration is done by migrating the GSA configuration over to the Mindbreeze format, but some configuration tasks remain.

To start configuration, click the Indices tab, click the Plus Sign to the left of Index Service, then check the box at the top right by Advanced Settings.

Figure 22. Indices configuration screen.



There are several fields on this screen to define. The following list should be investigated and completed as noted.

1. Index Node – Choose the node created previously from the drop-down list to assign the index service to that node.
2. Unrestricted Public Access – Check this box to prevent the index from authenticating users. Authentication is done differently on RDE, so unrestricted access needs to be enabled.
3. Query Services > Node – Check the box to the left of the node created previously to assign the query service to that node.
4. Data Sources – Migrating from a GSA config should create a default data source. Ensure that Category is Web, Category Instance is defined, and Source Name is defined as seen in Figure 23.

Figure 23. Index data sources.

Data Sources (1) ☐ Collapse all

Data Source	Access Node
ERDC Websites (Web)	search.erdcdren.mil

Setup

Category:

Category Instance:

Source Name:

Caching Principal Resolution Service:

Access Node:

Crawler Interval: hours

Crawler Schedule:

Web Page

Crawling Root
Crawling Root [1]: <input type="text" value="https://swwrp.usace.army.mil/"/>
Crawling Root [2]: <input type="text" value="http://www.wbdg.org/ccb/browse_cat.php?c=68"/>

In the Web Page section, each data source URL to be indexed is listed as a Crawling Root. To add new data sources, click the Add button at the bottom of the section. Below the crawling root entries, the URL Regex box contains the indexing rules for each URL as described previously in the configuration migration section. Each data source must have a regex entry added to this box. A working knowledge of Linux based regular expression syntax is required, but to direct the index service to crawl all content on the data source, use this regex form:

```
((?-i)\Qhttps://website.url.here.mil/\E.*)
```

If there is content that does not need to be indexed, add a regex exclusion rule to the list in the URL Exclude Pattern box.

5. User Agent – This is the user-agent string that the index service will present to the data source during crawling. For RDE authentication purposes, this must equal erdc-crawler. For other implementations, it will be specific to that network's requirements.

6. Max Document Size (MB) – This defines the maximum size of a file that the index service will collect; default is 50 MB. For this project, the value was increased to 100 MB.
7. Robots Honoring Policy – Choose “Obey all robot.txt rules for the configured user agent” from the drop-down list to force the index service to adhere to search etiquette defined on the data source.

Once all of these fields have been completed, check the box at the top to the left of `Apply changes and restart on save`, then click the `Save` button to restart the index service and apply the configuration changes.

Filters tab

Filters are used to modify, sort, and display indexed content in various ways. The filter service can perform very robust transformations of the data when configured to do so, but for this project, no special filters outside the defaults were created. Ensure that the correct Filter Service Node is selected and select filter plugins and properties as desired.

Client services tab

In simple terms, the client service is the web interface the end user sees when they want to perform a search query. The client service also handles search user authentication if desired. Mindbreeze delivers a default client service page with the appliance, but it is branded with their logo and colors; most customers will want a search page that looks and feels like their existing web pages. The ability to create a custom client service interface is included in the client service configuration.

To start configuration, click the `Client Services` tab, click the `Plus Sign` to the left of `Web Client Service`, then check the box at the top right by `Advanced Settings` (Figure 24).

Figure 24. Client services configuration screen.

The screenshot displays the 'Client Services' configuration page in the Mindbreeze Management Center. The left sidebar contains navigation links: Search Apps, Reporting, Search Experience, Services, Configuration, Setup, Update, and System. The main panel shows the 'Web Client Service' configuration. At the top, there's a 'Name' field with a '+ Add Client Service' button and a 'Disable' toggle. Below this, a 'Setup' section contains various configuration fields:

- Display Name:** Web Client Service
- Node:** search.erd.c.dren.mil
- Port (HTTPS):** 443
- Data Port (TCP/IP):** 23700
- Query Metrics Port (TCP/IP):** (empty field with note: leave empty to disable metrics servlet)
- Requires Authentication:** Yes
- Suppress Termination Cause:** ☒
- Display Tabs for Data Sources:** ☐
- Enable Tab Editing:** ☒
- Load More Results Using:** Pages
- Maximum Number of Displayed Pages:** 10
- URL of Help-Website:** http://inspire.mindbreeze.com/de/Cheat_Sheet.ht
- Fabasoft app telemetry Web API URL:** <http://localhost/web.telemetry>
- Dump Requests:** Never
- Dump Directory:** (empty field)
- One Phase Search and Enrich:** ☒
- Logout Redirect URL:** (empty field)
- User ID is E-Mail Address:** ☐

There are several fields on this screen to define. The following list of fields should be investigated and completed as noted.

1. Index Node – Choose the node created previously from the drop-down list to assign the index service to that node.
2. Requires Authentication – Several authentication methods are provided by Mindbreeze, and utilizing any of these methods requires choosing Yes from this drop-down list. If authentication is not utilized, then choose No.
3. Use SSL (HTTPS) – SSL is required on all DoD networks, so this box must be checked.
4. SSL Certificate – The SSL certificate installed previously should be listed in this drop-down list, so select the certificate from the list. If not listed, see additional SSL certificate instructions later in this document.
5. Use SAML Authentication – Security Assertion Markup Language (SAML) is an authentication standard that facilitates single sign on (SSO) functionality across websites. RDE provides SSO service utilizing Ping Federate software that adheres to the SAML standard. If SSO is desired, check this box, otherwise leave it unchecked.

6. External URL – Enter the server URL provided by RDE into this box.
7. Trusted Peer Communication to Query Services – If authentication is enabled on the client service, check the box next to Authentication Generates Trusted Peer Credentials, otherwise leave it unchecked.
8. Filters – Any filters defined on the Filters tab previously are listed here, including the default filters. Check the box next to each filter to be shown on the client service search page.
9. Web Applications Contexts Settings – This section is very important to customizing the client service look and feel. Default Context Path is the URL path that will map to an actual file path on the appliance file system. For this project, the desired URL path of <https://search.erdcdren.mil/apps/search> requires entering /apps/search in this box.

Next, click the Add Property button to continue customizing the client service. Re-enter the desired URL Path in the first box, then enter the actual file path where the new client service web page code resides, including HTML, JavaScript, and CSS files, in the File Path box. For this project, the file system path was /data/apps/search. Leave all other settings in this section at their defaults (Figure 25).

Figure 25. Custom client service configuration.

Web Applications Contexts Settings

Default Context Path

Additional Context + Add Property

Additional Context[1]	
URL Path	<input type="text" value="/apps/search"/>
File Path	<input type="text" value="/data/apps/search"/>
Override Existing Path	<input type="checkbox"/>
Allow Symlinks	<input checked="" type="checkbox"/>

Authenticated URL pattern

if Client Service requires authentication.

Login URL pattern

if Client Service authentication is optional.

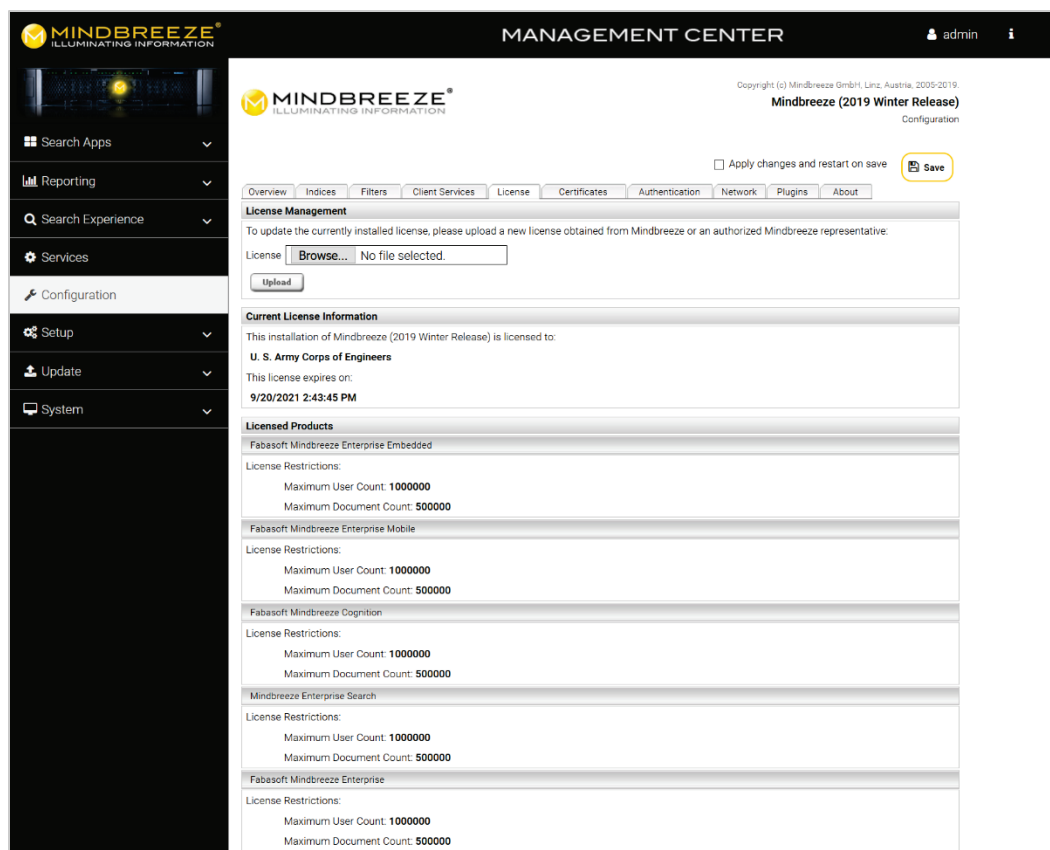
Once all of these fields have been completed, check the box at the top left of Apply changes and restart on save, then click the Save button to restart the client service and apply the configuration changes.

License tab

The Mindbreeze appliance requires a license to function, which will change in cost by the number of indexes desired. There are several levels of licenses starting at 500,000 documents up to unlimited documents. Additional hardware is required to go above 2,000,000 indexes. For this project, 500,000 indexes met ERDC's knowledge management requirements. The license is good for 3 years, and must be renewed through Onix for the appliance to continue operating.

Onix provides the license file via email attachment after payment is received. Save the attached license file and upload it to the appliance on the License tab as shown in Figure 26. License information will be displayed on this page following a successful file upload.

Figure 26. License management screen.



Certificates tab

In addition to the SSL certificate upload process described previously, there are more certificate management and configuration options on the Certificates tab. Trusted Certificate Authority (CA) files can be uploaded and managed, and trusted peer certificates can be assigned.

To upload an SSL certificate or CA file, use the Upload Certificates section. Choose the type of certificate from the drop-down box and browse to locate the certificate file. CA files are generally prepared in the .pem (<filename.pem>) file format, and SSL files in the PKCS12 (<filename.p12>) format. Successfully uploaded certificates and CAs are displayed in the sections below and can be seen in Figure 27. To remove a certificate, click the Trash Can icon on the right-hand side.

Figure 27. Certificates management screen.

MINDBREEZE
ILLUMINATING INFORMATION

MANAGEMENT CENTER

admin

Copyright (c) Mindbreeze GmbH, Linz, Austria, 2005-2019.
Mindbreeze (2019 Winter Release)
Configuration

Apply changes and restart on save **Save**

Overview Indices Filters Client Services License Certificates Authentication Network Plugins About

Upload Certificates

You can upload certificates used as **Trusted Certificate Authority**, as well as **SSL certificates** for the secure connection of your Client Service. To configure the certificate authority used for verification of peers, please upload the PEM-formatted file (<filename>.cer) containing the CA's certificate. To configure SSL certificates, please upload a PKCS 12 file (<filename>.p12).

Certificate: Auto **Browse...** No file selected.

Upload

Current Trusted CA Information

All trusted peers must present a valid SSL Certificate issued by:

None

Available CAs

Trusted Peer	Certificate Issuer	Certificate Subject	Expiration
<input type="checkbox"/>	CN=DoD Root CA 3, OU=PKI, OU=DoD, O=U.S. Government, C=US	CN=DoD Root CA 3, OU=PKI, OU=DoD, O=U.S. Government, C=US	12/30/2029 7:46:41 PM
<input type="checkbox"/>	CN=DOD SW CA-54, OU=PKI, OU=DoD, O=U.S. Government, C=US	CN=search.erdic.dren.mil, OU=USA, OU=PKI, OU=DoD, O=U.S. Government, C=US	5/9/2022 2:46:06 PM
<input type="checkbox"/>	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=GeoTrust RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	11/6/2027 7:23:45 AM
<input type="checkbox"/>	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	11/9/2031 6:00:00 PM

Available SSL Certificates

Certificate Issuer	Certificate Subject	Expiration
CN=DOD SW CA-54, OU=PKI, OU=DoD, O=U.S. Government, C=US	CN=search.erdic.dren.mil, OU=USA, OU=PKI, OU=DoD, O=U.S. Government, C=US	5/9/2022 2:46:06 PM
CN=SigningCert, OU=USA, PKI, DoD, O=ERDC, L=Vicksburg, S=MS, C=US	CN=SigningCert, OU=USA, PKI, DoD, O=ERDC, L=Vicksburg, S=MS, C=US	4/23/2020 11:35:11 AM
CN=GeoTrust RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=* erdc.dren.mil, O=Engineer Research and Development Center, L=Vicksburg, S=Mississippi, C=US	12/21/2019 6:00:00 AM

Once certificate management has been completed, check the box at the top left of **Apply changes and restart on save**, then click the **Save** button to restart and apply the configuration changes. To know when to update the certificate, make a note of the expiration date.

Authentication tab

Several methods of authentication are included with the Mindbreeze InSpire appliance. Kerberos, SAML, Central Authentication Service (CAS), Trusted Peer, and Basic Auth are all supported. For this project, SAML and SSO were required. RDE provides SSO service utilizing Ping Federate software that adheres to the SAML standard.

Start the SSO implementation process by contacting RDE to enter a new request ticket including the server URL and SSL certificate provided previously by RDE. RDE will create a new site in Ping Federate using the supplied information and export a SAML identity provider file in the SAML 2.0 XML format. Upload that XML file to the Mindbreeze using the **Upload New SAML Identity Provider File** section as shown in Figure 28. Browse to locate the XML file, then choose the appropriate SSL certificate from the drop-down list and click the **Upload** button.

Figure 28. SAML configuration.

The screenshot displays the Mindbreeze Management Center interface for SAML configuration. The left sidebar contains navigation links: Search Apps, Reporting, Search Experience, Services, Configuration, Setup, Update, and System. The main content area is titled 'MANAGEMENT CENTER' and shows the 'ERDC Websites (Query Plugin) search.ercd.dren.mil' configuration. The 'Upload New SAML Identity Provider File' section includes a 'Browse...' button and a 'Choose Cert' dropdown menu set to 'Default SSL Certificate'. Below this is the 'SAML ID Status' section, which states 'A valid SAML identity file is installed.' The 'Available SAML Authenticators' section shows a table with one entry: 'https://search.ercd.dren.mil:443' with a certificate 'CN=search.ercd.dren.mil, OU=USA, OU=PKI'. The 'SAML Settings' section includes 'Session timeout' (30 min) and 'Metadata timeout' (7 days). The 'Enable/Disable SAML Authentication' section shows a table with 'Web Client Service' and 'search.ercd.dren.mil' with a checkbox checked and a dropdown set to 'https://search.ercd.dren.mil:443'.

An entry will appear in the **Available SAML Authenticators** section after successfully uploading.

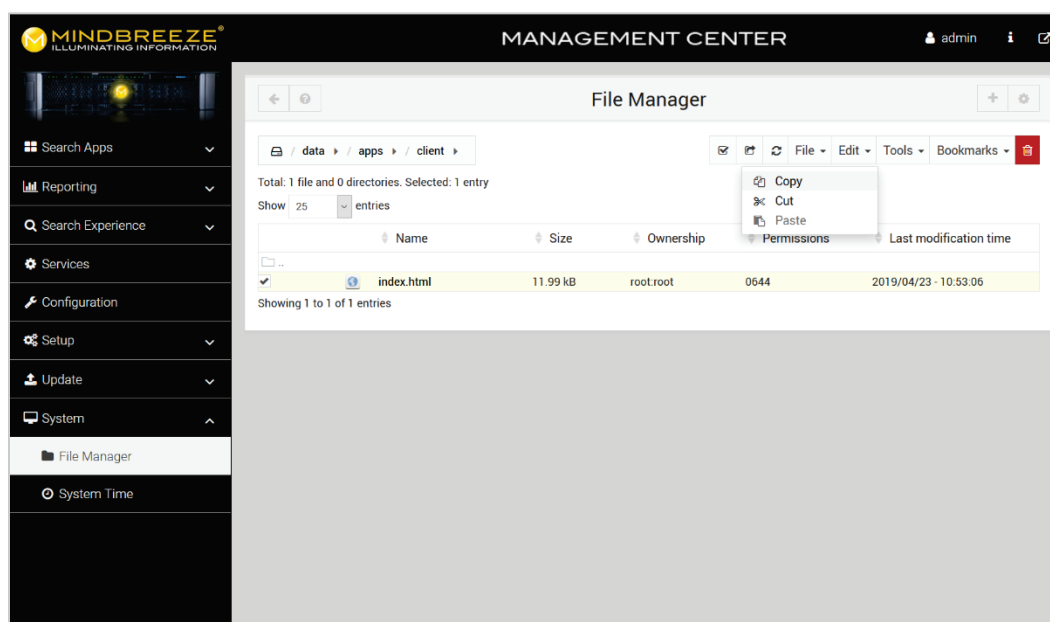
Next, in the Enable/Disable SAML Authentication section, check the box and select the SAML authenticator from the drop-down to enable SAML on the client service. Once SAML configuration is completed, check the box at the top left of Apply changes and restart on save, then click the Save button to restart the client service and apply the configuration changes. Visitors to the search client page will then be prompted to enter their CAC information before being allowed to enter and perform search queries.

Customizing the client service

A custom client service is necessary to ensure a better experience for end users. After configuring the client service to point to another file system path, customized files must be placed in that path for the client service to work properly. A working knowledge of HTML, JavaScript, and CSS is required to customize the client service files.

Start by using the File Manager to copy the default client service file into the newly configured custom folder. For example, previously the file path /data/apps/search was configured to be the custom client service folder. Copy the file index.html located in the /data/apps/client to the custom client service folder using the Edit menu in the File Manager as shown in Figure 29.

Figure 29. Copy file using file manager.



Use the File menu in File Manager to create a new directory in the /data/apps folder called search, then paste the copied file into the new directory.

Next, locate the default CSS file to begin customizing the page's stylesheet to better match existing branding. One option to accomplish this task is to save the stylesheet from the browser prior to changing the default client service path. A second method is to log in to the appliance's shell and copy the file to the custom client file folder. The default CSS file is located at /opt/mindbreeze/bin/webapps/client-service/ROOT/apps/css/adapted.css. Note that this method requires root access to the operating system and an SSH client to accomplish.

Once the style sheet file has been copied, edit the index.html file to point to the new file in the following manner.

Original line

```
<link href="../../../css/adapted.css?19.0.4.258" rel="stylesheet">
```

New line

```
<link href="adapted.css?19.0.4.258" rel="stylesheet">
```

Editing the default stylesheet is discouraged since many of the page layout styles are inside. The recommended method of custom styling is creating a new stylesheet file called custom.css in the same folder that includes CSS declarations that override or add to the original styles. Ensure the custom stylesheet line in index.html is pointing to the correct path, and make whatever styling changes required to the custom.css file.

Continue making HTML, CSS, or JavaScript modifications to the files until a satisfactory custom client is completed with matching branding and required features. The default client HTML also includes many convenience features for search users that can be retained or commented out with comment tags if they are determined not to be necessary. Figure 30 shows an example of ERDC's customized client service.

Figure 30. ERDC's customized client service.

The screenshot displays the ERDC (Engineer Research & Development Center) search interface. At the top, the 'SEARCH ERDC' logo is visible, with 'ENGINEER RESEARCH & DEVELOPMENT CENTER' written below it. A search bar contains the text 'Information Technology'. Below the search bar, it indicates 'About 9400 Results'. The results are listed in a grid format, each with a thumbnail image on the left and a text description on the right. The first result is titled 'Chief Information Officer (CIO)' and includes links to 'Open', 'Preview', and 'Collect'. The second result is titled 'Mobile Information collection application (MICA)' and also includes 'Open', 'Preview', and 'Collect' links. The third result is titled 'Mobile Information Collection Application (MICA)' and includes the same links. The fourth result is titled 'Big Data Informed Decision Making_v1.0.pptx' and includes 'Open', 'Preview', and 'Collect' links. On the right side of the results, there is a 'Sort by' dropdown menu set to 'Relevance', and a list of filters: 'Sources', 'Date', 'Category', and 'File type', each with a toggle switch.

SEARCH ERDC
ENGINEER RESEARCH & DEVELOPMENT CENTER

Information Technology

About 9400 Results

Chief Information Officer (CIO)
Open - Preview - Collect
9/9/19 8:23 AM
Chief Information Officer (CIO) - Inside...ERDC Wiki Chief Information Officer (CIO) From...CIO 2Chief Information Officer 3Deputy Chief Information Officer 4Accomplishments...oversight of ERDC Information Technology4.1.1Cybersecurity and Information Assurance 4.1...oversight of ERDC Information Technology With over 40...as over 200 Information Technology Acquisition System (ITAS)

Mobile Information collection application (MICA)
Open - Preview - Collect
9/9/19 8:23 AM
Mobile information collection application (MICA...ERDC Wiki Mobile information collection application (MICA...MICA Repurposing Information Assurance 9Wrap...today's Smartphone technologies can be used...capture field asset information in ways never...decision makers the information they needed to make informed, timely decisions. How...of Engineers - Information Technology (ACE-IT) group

Mobile Information Collection Application (MICA)
Open - Preview - Collect
9/9/19 6:13 AM
Mobile Information Collection Application (MICA...ERDC Wiki Mobile Information Collection Application (MICA...today's Smartphone technologies can be used...capture field asset information in ways never...with the Mobile Information Collection Application (MICA...decision makers the information they needed to make informed, timely decisions. How...of Engineers - Information Technology (ACE-IT) group

Big Data Informed Decision Making_v1.0.pptx
Open - Preview - Collect
9/9/19 4:42 AM - Title: Slide 1 - Author: bllmemb6 - Company: US Army - Version: 209 - Slides: 16 - Paragraphs: 281 - Words: 1779 - Presentation format: On-screen Show (4.3)
Big Data Informed Decision Making Reed...Mosher, PhD Director Information Technology Laboratory 06 May...global coupled ensemble technologies will provide increased

Sort by: Relevance

Sources: [x]
Date: [x]
Category: [x]
File type: [x]

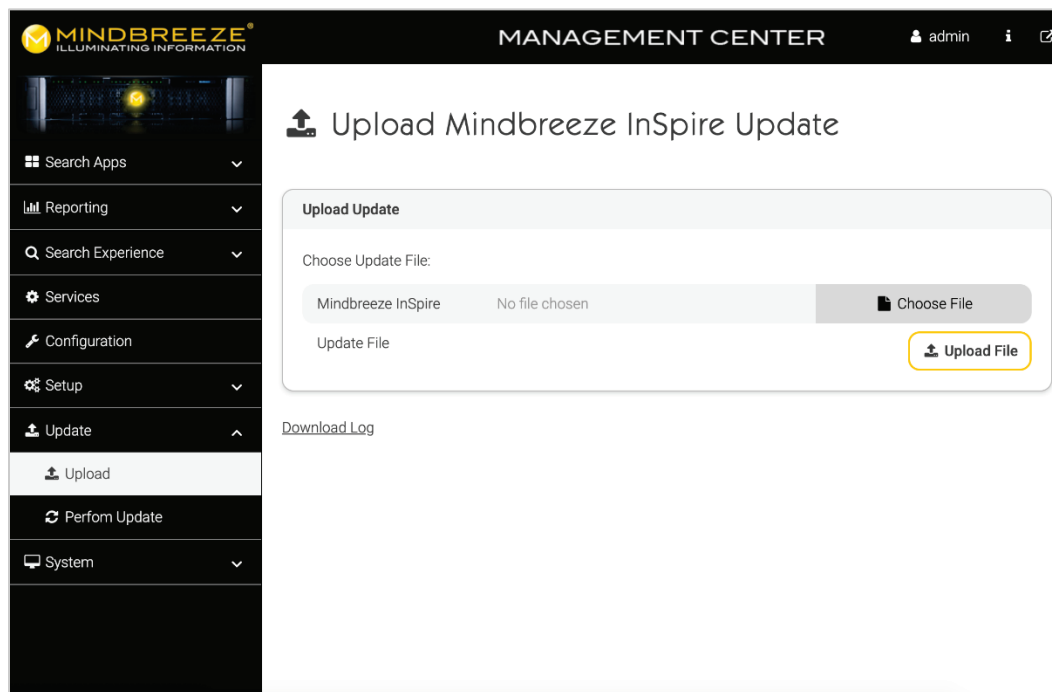
5 Maintenance

Software updates

As with any system, the search appliance must be maintained as new software is produced by Mindbreeze. Major software updates are released seasonally, which are titled by the season and year in which they are announced along with a version number. At the time of this report, the most recent update is the Winter 2019; release version 20.2.

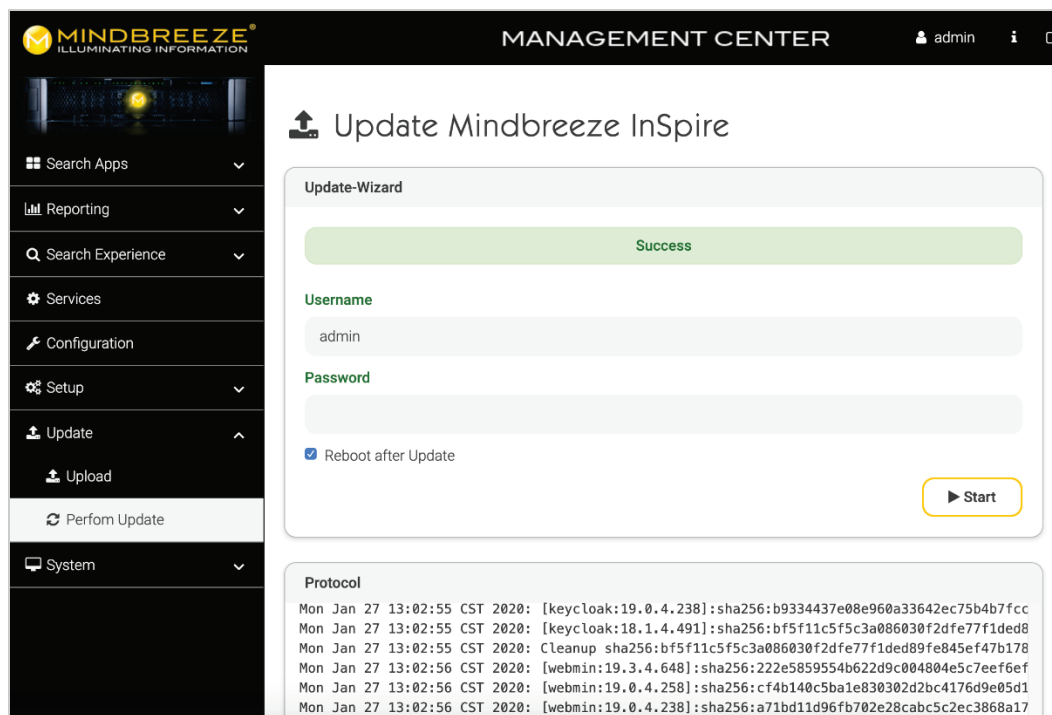
Updating the appliance with new software is a three-step process. First, the latest release must be downloaded to your local computer, which is available for download on the Mindbreeze website at <https://www.mindbreeze.com/inspire-updates.html>. Enter the requested information, then download the file which is in .zip format. Second, the file then must be uploaded to the search appliance via the management console as shown in Figure 31. Choose the file on the local computer, then click Upload File.

Figure 31. Upload Mindbreeze update.



Lastly, the update is executed by clicking on Perform Update in the left side menu bar. Enter the admin user name and password, then click Start. The results of a successful update are shown in Figure 32.

Figure 32. Software update success.



Depending on the size of the update, the update process can take a while to execute. After completion of the update, the appliance will restart automatically.

There are some things to consider before applying updates. Mindbreeze occasionally updates the operating system along with the InSpire software, so any changes made at the operating system level are at risk of being overwritten. If changes have been made, make a note of them or make backups of files that may be affected. In this case, a backup was made of the custom search interface, even though it is not at the operating system level.

Indexes

As the knowledge base at ERDC is expanded, new data sources (indexes) will need to be added to the list of indexes in the management console. Maintaining the list of data sources is handled on the Indices tab in the management console as previously described. Follow the instructions in

the Indices Tab section to add new data sources or remove those that are no longer active.

Certificate and license

SSL certificates have an expiration date when they are created. Typically, they are 3-5 years from the date of creation, but they can be shorter or longer in duration. The certificate upload process is described previously in this document in the **Certificates** Tab section. Use that process to upload a new certificate prior to the expiration date of the original one. Failing to do this before expiration will result in the loss of access to the search interface by users.

The license file provided by Mindbreeze at the time of appliance purchase also has an expiration date. This file must be maintained prior to expiration, or the appliance will fail to operate. The default expiration date is three years from the date of initial purchase. A new license must be purchased from the distributor Onyx as mentioned in the **Acquisition** section of this document. Use the process mentioned in the **License** Tab section of this document to upload the newly acquired license file to the appliance.

6 Backup Strategies

Two Mindbreeze InSpire appliances were purchased with the intention of having a stand-by appliance in case of a failure with the main one.

Mindbreeze does offer the capability to mirror two appliances, so one can fail without an interruption in service, but to accomplish this, additional hardware is required. This knowledge was not communicated during the purchase process, so the required hardware was not purchased.

As a result, a “plan B” strategy was developed. The second Mindbreeze appliance was configured as closely as possible to the state of the first one, and kept in reserve as a “warm backup.” This terminology means the second appliance has most of the configuration needed to be deployed in case of a failure, but some setting will need to be made after the original appliance is offline. For example, the IP address of the first appliance cannot be duplicated on the network, so the second appliance will need to be assigned that IP after the first one is removed from the network. Other last-minute settings include the SSL certificate, license file, and SAML authentication. These settings cannot be configured identically on two appliances on the network at the same time. All other settings such as indexing and search interface can be configured, so the amount of work to bring the second appliance online in case of the original one failing is significantly reduced.

Future hardware upgrades should include the purchase of items required to produce a true “hot backup” environment to reduce the backup switch time to near zero. This possibility will be evaluated with the vendor when the license renewal is due.

7 Lessons Learned

Throughout the processes of acquisition, installation, and configuration, several important lessons were learned. These lessons can be applied to future implementations of Mindbreeze InSpire search appliances within the ERDC, U.S. Army Corps of Engineers, or the greater Department of Defense (DoD).

Acquisition

As mentioned previously, Mindbreeze is a company based in Austria. While that doesn't necessarily preclude purchasing directly from them, the process for making a purchase internationally is certainly more complicated than purchasing domestically. Having Onix in the U.S. to facilitate the purchase made the process much simpler. They have experience with the federal acquisition processes and are affiliated with several acquisition vehicles. Assuming they maintain their status as a Mindbreeze distributor, purchasing in the future will remain simple. If their status changes, acquisition may become more difficult.

Keep in mind that ERDC logistics can be fairly slow when processing purchasing arrivals. Around two months should be added to the timeline to account for logistical holdups.

Installation

Installation required close collaboration with RDE to complete. Depending on the network host being used, the amount of time and effort to install may be increased. While RDE will run network cables, they will not configure the iDRAC or other connections. As described previously, physical access to the appliance is required to configure the iDRAC connection. This means that access was needed to a secure computing room. The process for acquiring access took around two weeks to complete, which involved an application that had to be routed through the management chain and CAC programming. This is probably true for every computing room across the DoD, so keep this in mind.

When configuring IP addresses for the appliance's network interfaces, any changes to this information forces a reboot of the appliance. A wait time of several minutes follows, and if the IP was entered incorrectly, the iDRAC is

the only way to communicate with the appliance again. This lesson was learned the hard way, so double check the IP entries before continuing.

Configuration

During search client customization, root access to the appliance operating system is required to gain access to the default client CSS after changing the search interface path. To gain root access, the default password is required. Mindbreeze does not supply the root password without attending their in-person training course first. The Mindbreeze Certified Expert training is conducted domestically in Chicago, IL periodically throughout the year. They have teamed with Onix to give the U.S. Government customers a way to easily purchase the training. After training, they provide the root password. Keep this requirement in mind when planning for appliance implementation.

Mindbreeze tech support is located in Austria. Onix provides basic support for the appliance, but if more advanced support is needed, Mindbreeze is the only option. When scheduling support calls or remote support, keep in mind that Austria is in the Central Europe Standard Time (CEST) zone. CEST can be easily confused with Central Standard Time (CST) when accepting support invitations.

In a large environment with multiple servers and massive amounts of knowledge to be aggregated, splitting duties over multiple nodes is recommended. In ERDC's knowledge environment, it was not necessary to configure the appliance in this manner. Indexing and client services can run comfortably within one node. Future implementations may need to consider splitting duties over multiple nodes if the amount of knowledge increases significantly.

When uploading an SSL certificate to the appliance, the software, by default, will automatically try to determine the certificate type. This automatic determination did not work as expected. There is an option to choose the type of certificate manually, and doing this resulted in success. Always choose the certificate type when uploading to ensure the certificate is uploaded and installed properly.

An issue was discovered when setting up the SAML authentication that required Mindbreeze support. When the SSO service sent the authentication token back to the appliance, the request was not being

processed properly, which resulted in a failed log in. Further inspection by support identified a problem with the software not redirecting the request to the proper end point on the appliance. An operating system change was made to modify the hosts file to handle the redirect. Hopefully in future software updates, this issue will be fixed.

Implementing the Minbreeze InSpire search appliance was a complicated, and at times tedious process, but it was necessary to maintain ERDC's core knowledge management requirements when Google ended their search appliance product. Expect to have Onix and Mindbreeze support help with issues that arise, because issues will arise. Their support is timely and are always helpful. A remote session, which is an option provided at no extra charge, was required to find the SAML issue.

Acronyms and Abbreviations

API	Application Programming Interface
CSED	Computational Science and Engineering Division
CSS	Cascading Style Sheet
DNS	Domain Name Service
ERDC	Engineer Research and Development Center
GSA	Google Search Appliance
HTML	Hypertext Markup Language
HTTP(S)	Hypertext Transfer Protocol (Secure)
iDRAC	Integrated Dell Remote Access Controller
IP	Internet Protocol
ITL	Information Technology Laboratory
LCD	Liquid Crystal Display
MAC	Media Access Control
NIC	Network Interface Card
ORTT	Office of Research and Technology Transfer
PKI	Public Key Infrastructure
RDE	Research and Development Environment
SAML	Security Assertion Markup Language
SSL	Secure Sockets Layer
SSO	Single Sign On
URL	Uniform Resource Locator
XML	Extensible Markup Language

REPORT DOCUMENTATION PAGE*Form Approved*
OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. **PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.**

1. REPORT DATE (DD-MM-YYYY) September 2020		2. REPORT TYPE Final		3. DATES COVERED (From - To)	
4. TITLE AND SUBTITLE Mindbreeze InSpire Search Appliance Implementation and Lessons Learned				5a. CONTRACT NUMBER	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S) Byron M. Garton, Jonathan S. Broderick, and Michael A. Clement				5d. PROJECT NUMBER	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Information Technology Laboratory U.S. Army Engineer Research and Development Center 3909 Halls Ferry Road Vicksburg, MS 39180-6199				8. PERFORMING ORGANIZATION REPORT NUMBER ERDC/ITL SR-20-15	
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) ERDC Office of Research and Technology Transfer (ORTT) 3909 Halls Ferry Road Vicksburg, MS 39180-6199				10. SPONSOR/MONITOR'S ACRONYM(S)	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited.					
13. SUPPLEMENTARY NOTES ERDC Office of Research and Technology Transfer (ORTT), WIC 19F1H5					
14. ABSTRACT The U.S. Army Engineer Research and Development Center (ERDC) Knowledge Management relies on enterprise search technology to index and search ERDC's accumulation of knowledge stored on various web connected systems. In 2016, Google announced the discontinuation of their search product, the Google Search Appliance (GSA), at the end of March 2019. After conducting extensive market research and identifying a suitable replacement that met all ERDC requirements, a competing product called Mindbreeze InSpire was chosen. This product provides a simple-to-use interface that facilitates quick location and retrieval of ERDC knowledge located on ERDC's internal and extranet websites, and is designed for simple and intuitive installation and configuration. This document investigates and details the acquisition, installation, and configuration of the Mindbreeze InSpire enterprise search appliance, and the lessons learned throughout the entire implementation process.					
15. SUBJECT TERMS Knowledge management		Search engines – Evaluation			
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT SAR	18. NUMBER OF PAGES 49	19a. NAME OF RESPONSIBLE PERSON
a. REPORT Unclassified	b. ABSTRACT Unclassified	c. THIS PAGE Unclassified			19b. TELEPHONE NUMBER (include area code)