ESN 1.0
Administrative User Interface Reference

January 2017

Legal Notice

For information about legal notices, trademarks, disclaimers, warranties, export and other use restrictions, U.S. Government rights, patent policy, and FIPS compliance, see https://www.novell.com/company/legal/.

Contents

About This Guide

This guide is for ESN 1.0 administrators and covers the administrative dialogs and screens for the following services and features:

Audience

This guide is intended for ESN administrators.

Feedback

We want to hear your comments and suggestions about this manual and the other documentation included with this product. Please use the **comment on this topic** link at the bottom of each page of the online documentation.

Documentation Updates

For the most recent version of the *Micro Focus ESN Administration Guide* and other documentation, visit the Micro Focus ESN 1.0 Documentation website (http://www.novell.com/documentation/esn-1).

Additional Documentation

You can find more information in the Micro Focus ESN documentation, which is accessible from the Micro Focus ESN 1.0 Documentation website (http://www.novell.com/documentation/esn-1).

1 Administrative Consoles

Port 9443 Appliance Console

Path: https://*appliance_ip_or_dns*:9443

- You and those with the `vaadmin` or `root` user password use this to manage virtual-machine-level settings and ESN service configurations that affect an entire service and its interactions with other services.

Figure 1-1 *The Port 9443 ESN Console*
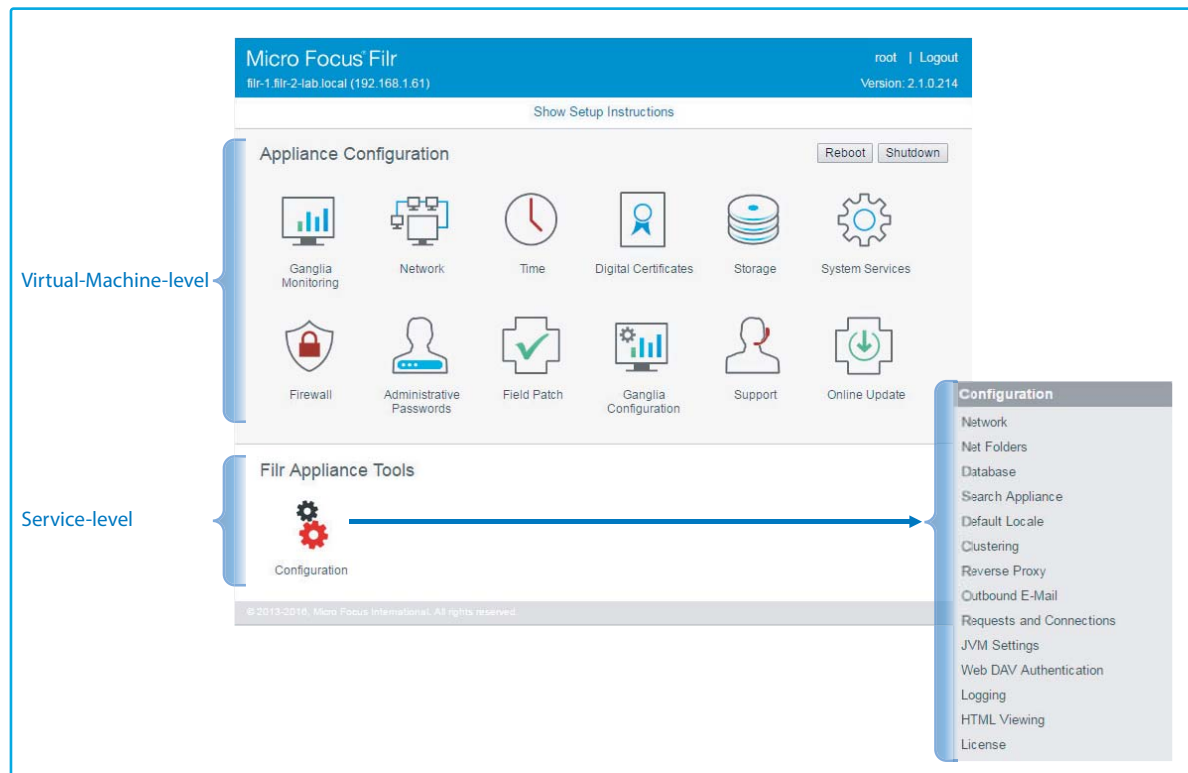
Port 8443 ESN Administration Console

Path: https://*appliance_ip_or_dns*:8443 > *Username* > **Administration Console**

- You and other designated ESN administrators use this console to manage all aspects of ESN services.
- If the ESN appliance is configured for port redirection, ESN users, including administrators, might not need to include the port number.
- If ESN is configured to use NetIQ Access Manager, the ESN login screen is not used. For more information about ESN configurations that affect login, see "Changing Network Settings" on page 47.

Figure 1-2   *The Port 8443 ESN Console*
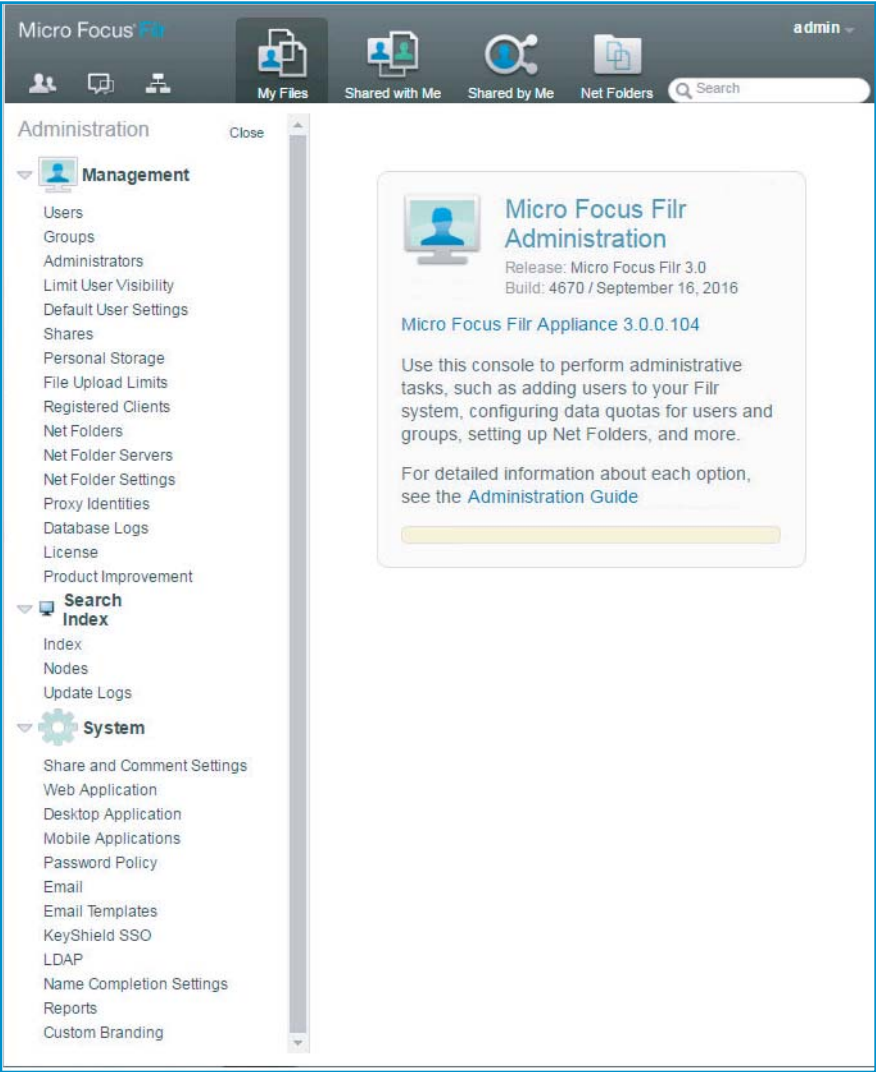
2 Administrative Access

This section covers the following ESN administrator-related tasks:

- "Assigning and Managing Port 8443 Designated Administrators" on page 11
- "Changing Passwords and SSH Access for vaadmin and root" on page 12
- "Logging In as an Administrator" on page 12

For more information about ESN administrators, see "ESN Administrative Users" in the *ESN 1.0: Understanding How ESN Works* guide.

Assigning and Managing Port 8443 Designated Administrators

Path: Port 8443 ESN Admin Console **Management > Administrators**

Best Practice: You can plan your Designated Administrators in advance or create them as needs develop. In either case, you should keep a record of those with administrative access on this worksheet:

- Worksheet 19 - Administrative Access

Table 2-1 *Using the Manage Administrators dialog*

Field, Option, or Button	Information and/or Action
About Port 8443 Direct Administrators	Port 8443 Designated Administrators can only administer the following: • Users • Groups • Mobile Devices
Administrators	
• **Add**	1. Click **Add** to add a new Designated Administrator. 2. Begin typing the user or group name you want to assign. 3. Click a user or group to add it to the list.
• **Remove**	1. Select one or more users or groups in the **Administrators** list. 2. Click **Remove**. The selected items are removed.

Field, Option, or Button	Information and/or Action
◆ **Filter** list	1. Type an alphanumeric string contained in the user or group names you want to display. 2. Press Enter. The list displays only the names that contain the string you entered.
◆ Gear icon	1. Click the icon 2. Select **Edit Column Sizes**. 3. Follow the instructions in the Edit Column Sizes dialog to adjust column widths. Changes persist from session to session.

Changing Passwords and SSH Access for vaadmin and root

NOTE: Changing both passwords requires logging in as `root`. If you log in as `vaadmin`, you can only change the `vaadmin` password.

Path: Port 9443 Appliance Console **Administrative Passwords**

Table 2-2   The Administrative Passwords dialog

Field, Option, or Button	Information and/or Action
vaadmin	◆ Acting as either `vaadmin` or `root`, type the current password, type and confirm the new password, and click **OK**.
root	◆ Acting as `root`, type the current password, type and confirm the new password, and click **OK**.
root SSH Access	◆ Acting as `root`, select or deselect **Allow root access to SSH** and click **OK**. SSH is disabled by default. For information about how to start SSH on the appliance, see Chapter , "Managing System Services," on page 87.

Logging In as an Administrator

Port 8443 Console

Path: Port 8443 ESN Admin Console

Table 2-3 *Using the Sign In dialog*

Field, Option, or Button	Information and/or Action
◆ **User ID:**	◆ **First-time login:** The username you specified in "Specify the First Search Appliance, Locale, and Admin user" in the *ESN 1.0: Installation, Deployment, and Upgrade Guide*. The default is admin. ◆ **Subsequent login:** The name of the built-in ESN administrator (default is admin), or a directly assigned administrator.
◆ **Password:**	◆ **First-time login:** Enter the username. You are then prompted to change the password. ◆ **Subsequent login:** Administrative user password set above or changed in the Profile.
◆ **Change Password**	◆ **First-time login only** 1. Type the current password, which is the username. 2. Type and confirm a new, more secure password.

Port 9443 Console

Path: Port 9443 Appliance Console

Table 2-4 *Port 9443 Sign In dialog*

Field, Option, or Button	Information and/or Action
◆ **Username**	◆ Enter either vaadmin or root.
◆ **Password**	◆ Type the password for vaadmin or root

3 Access to ESN and Its Services

Users can access ESN through web browsers, desktops, and mobile devices.

- "Desktop Access—Default Settings" on page 15
- "Desktop Access—Individual Users and Groups" on page 17
- "Mobile Device Access—Default Settings" on page 18
- "Mobile Device Access—Individual Users and Groups" on page 20
- "Web Browser Access—Default Settings" on page 23
- "Web Browser Access—Individual Users and Groups" on page 23

Desktop Access—Default Settings

Settings made here apply to all ESN users unless ESN access and password caching are overridden by settings made through the Users or the Groups management dialogs.

Path: Port 8443 Appliance Console **> System > Desktop Application**

Table 3-1   Using the Configure Desktop Application dialog

Field, Option, or Button	Information and/or Action
Allow Desktop Applications to:	
◆ **Access ESN**	◆ Select this to allow all users to access ESN through the ESN desktop application.
	◆ Deselect this if you want only designated users and groups to have desktop access as controlled through user and group settings
◆ **Cache the user's password**	◆ Select this to allow users to enable the **Remember password** option on the **Account Information** page in the Micro Focus ESN Console.
	Remember password option availability is also configurable for individual users and groups through the Users and the Groups management dialogs (**More > Desktop Application Settings**).
◆ **Be deployed**	◆ Select this to expose the Download ESN Desktop App option in the web client > user drop-down menu.
	Alternatively, you can download the desktop apps from download.novell.com and distribute them using client management software such as Micro Focus ZENworks.
	For more information, see "Client Management Software and the ESN Desktop Applications" in the *ESN 1.0: Maintenance Best Practices Guide*.
◆ **Deploy files contained locally**	◆ Select this to allow users to download the Desktop App contained in ESN.

Field, Option, or Button	Information and/or Action
◆ **Deploy files accessed via URL to another location**	◆ Select this and specify the URL of the server that is hosting the Desktop App downloads. To set up web server distribution of the desktop app, see "Hosting Desktop Application Installation Files on a Separate Server" in the *ESN 1.0: Maintenance Best Practices Guide*. ◆ This is required if your ESN system is fronted by an L4 or L10 switch. ◆ This is a best practice because it minimizes the load on ESN.
Desktop Synchronization	
◆ **Synchronize every __ Minutes**	◆ Specify how many minutes you want the desktop app to wait after a desktop synchronization ends before it checks again for changes to **Available Offline** files. Default=15 minutes. ◆ You can use this to control the synchronization load that the ESN desktop application puts on ESN. ◆ Changes on the desktop are automatically synchronized to ESN regardless of this setting.
◆ **Maximum file size that can be synchronized:**	◆ Specify the maximum file size (in MB) that can be synchronized between the ESN desktop application and ESN.
◆ **Remove cached files after X days**	◆ Specify the number of days that locally cached files remain on users' desktops after they are no longer being accessed or modified.
◆ **Allow user to modify cached files lifetime**	◆ Select this to allow users to specify how long they want locally cached files remain on their desktops after the files are no longer being accessed or modified.
Application Whitelist/Blacklist	For more information, see "Controlling File Downloads by the ESN Desktop Applications" in the *ESN 1.0: Maintenance Best Practices Guide*.
◆ **Restore Defaults...**	◆ Click this to restore the defaults for all settings in the Application Whitelist/Blacklist section below.
Mode	◆ Lets you control how antivirus, backup, and other applications download files that are accessible through ESN.
◆ **No restrictions - Ignore the lists.**	◆ Select this if you want all applications, including antivirus scanners and backup software, to download files to the workstation's local disk.
◆ **Whitelist - Allow only the listed applications to download files.**	◆ If you select this, then download attempts by unlisted applications trigger system alerts to users that a download has been "blocked by an administrative setting." This option doesn't provide for user control of application-driven downloads. ◆ Whitelists are empty by default. ◆ You can add and remove applications for your organization as needed.

Field, Option, or Button	Information and/or Action
◆ **Blacklist - Block the listed applications from downloading files.**	◆ If you select this, then download attempts by blacklisted applications trigger system alerts to users that a download has been "blocked by an administrative setting."
	This option doesn't provide for user control of application-driven downloads.
	◆ ESN includes two default blacklists (Windows and Mac) that you can modify as needed.
	◆ Blacklisted applications are blocked from downloading files through ESN.
	◆ Unlisted applications are allowed to download files.
◆ **Whitelist and Blacklist - Allow and block the listed applications. Prompt users to allow or block unlisted applications.**	◆ If you select this option, then
	◆ Blacklisted applications are always blocked.
	◆ Whitelisted applications are always allowed.
	◆ A download attempt by an unidentified application causes the application to be added to a list of blocked applications.
	◆ Users can allow downloading by any blocked applications through their desktop ESN console.
Whitelist	◆ This is empty by default.
	◆ Only the built-in administrator can create a customized list.
	◆ Applications listed here and in the Blacklist are blocked.
	In other words, the Blacklist trumps the Whitelist.
Blacklist	◆ ESN includes a fairly extensive list of common antivirus and backup applications to offer a level of protection against unwanted file downloading.
	◆ Only the built-in administrator can customize this list.
OK button	◆ Click this to save your changes.
	Current user sessions are not affected. To see changes, users must log in to a new session.
Cancel button	◆ Click this to cancel the changes you have made.

Desktop Access—Individual Users and Groups

Path: Port 8443 Appliance Console Management > Users/Groups > *select one or more users* or *groups* > **More > Desktop Application Settings...**

Table 3-2   Using the Configure Desktop Application dialog (applies in both user and group contexts)

Field, Option, or Button	Information and/or Action
Configure Desktop Application (*X* users)	
Use default settings option	◆ Select this to apply all of the settings in the Configure Desktop Application dialog to the selected users or groups.

Field, Option, or Button	Information and/or Action
Use user settings to allow the desktop application to: option	◆ Select this to apply the access and password caching settings below to the selected users or groups. The following two settings override their counterparts in the Configure Desktop Application dialog and all other settings there apply here.
◆ **Access ESN**	◆ Selecting this allows the previously selected users or groups to access ESN through the ESN desktop application. ◆ Deselecting this option blocks the previously selected users or groups from accessing ESN through the ESN desktop application.
◆ **Cache the user's password**	◆ Selecting this allows the previously selected users or groups to enable the **Remember password** option on the **Account Information** page in the Micro Focus ESN Desktop Console. ◆ Deselecting this blocks the previously selected users or groups from enabling the **Remember password** option on the **Account Information** page in the Micro Focus ESN Desktop Console.
OK button	◆ Click this to save your changes. Current user sessions are not affected. To see changes, users must log in to a new session.
Cancel button	◆ Click this to cancel the changes you have made.

Mobile Device Access—Default Settings

Path: Port 8443 ESN Admin Console**System** **> Mobile Applications**

Table 3-3 *Using the Configure Mobile Applications dialog*

Field, Option, or Button	Information and/or Action
Allow mobile applications to:	
◆ **Access ESN**	◆ Select this to allow access to ESN through ESN mobile apps.
◆ **Cache the user's password**	◆ Select this to let users enable the **Save Password** option when logging in to the ESN site through a ESN mobile app.
◆ **Allow files to be added to the Downloads area for offline access**	◆ Select this to let users download files from ESN to mobile devices. **IMPORTANT:** If you don't want users downloading files, make sure that you also disable downloading through web browsers. ◆ Downloaded files can be viewed in offline mode by accessing the **Downloads** section in the app. ◆ Users are responsible for the security of downloaded files. See "Encrypting Downloaded Files" in the "Micro Focus ESN Mobile App 1.0 Quick Start".
◆ **Force PIN Code**	◆ Select this to force users running version 2.0 and later mobile apps to have a 4-digit access code set on their devices for accessing ESN See "Configuring a 4-Digit Passcode" in the "Micro Focus ESN Mobile App 1.0 Quick Start."

Field, Option, or Button	Information and/or Action
◆ **Cut/Copy**	◆ Select this to let users cut or copy data from the ESN mobile app so that the data can be pasted into third-party applications.
◆ **Screen capture (affects Android only)**	◆ Select this to let users take a screen capture while inside the ESN application. **IMPORTANT:** As noted in the option name, this only applies to Android devices. iOS users can always take screen captures.
◆ **Disable applications on rooted or jail-broken devices**	◆ Select this to prevent users from running the ESN mobile app on devices that have been rooted or jail-broken.
Open in: drop-down list	◆ Click the drop-down list and select the option that is best for your organization as described in the rows below. ◆ This controls whether users can open files in third-party apps through ESN. For example, a user views a file in ESN, opens and modifies the file in a document editing app, then saves the file back to the ESN app. ◆ iOS calls this "Open In" functionality; Android devices refer to it as "Share" or "Send To." **IMPORTANT:** For MobileIron device management, the following points apply: ◆ In almost all cases the ESN and MobileIron settings must be consistent with each other. ◆ The exception is if you want only the MobileIron-managed devices to have Open In capabilities. To cause this behavior, 1. Enable Open In in MobileIron. 2. Disable Open In in ESN.
◆ **Disabled** option	◆ This prevents users from opening files in ESN using third-party applications.
◆ **All applications** option	◆ This lets users open files in ESN using any third-party application.

Field, Option, or Button	Information and/or Action

◆ **Whitelist** option	◆ This opens two Whitelists (Android and iOS) of third-party apps that users are allowed to open files into.
	
	IMPORTANT
	
	  ◆ Only Android package names and iOS bundle IDs are valid list entries.
	
	  ◆ To get an Android app package name:
	
	    1. Install the `Package Name Viewer` app from the Google Play store.
	      This app displays the package name for each app that is currently installed on the device.
	
	  ◆ To find the bundle ID for an iOS app:
	
	    1. Synchronize the app to iTunes from your device.
	
	    2. In the iTunes library, open the `Mobile Applications` folder.
	      For iTunes on Mac, the default location is your Home directory at: `~/Music/iTunes/Mobile Applications/`
	      For iTunes On Windows, the default location is `C:\Users\`*username*`\My Music\iTunes\Mobile Applications/`
	
	    3. Create a copy of the app's file, and re-save the copy as a `.zip` file.
	
	    4. Unzip the newly created `.zip` file.
	      You now see a folder by the name of the application name.
	
	    5. Locate the `iTunesMetadata.plist` file within the folder and open it in a text editor.
	
	    6. The bundle ID is the string displayed below the `softwareVersionBundleid` key within the file.

Mobile synchronization	
◆ **Synchronize every X Minutes**	◆ Specify how many minutes the mobile apps wait after a desktop synchronization ends before they start another synchronization with ESN. Default=15 minutes. ◆ You can use this to control the synchronization load that the ESN mobile app puts on ESN.
OK button	◆ Click this to save your changes. Current user sessions are not affected. To see changes, users must log in to a new session.
Cancel button	◆ Click this to cancel the changes you have made.

Mobile Device Access—Individual Users and Groups

Path: Port 8443 ESN Admin Console**Management > Users/Groups >** *select one or more users* **or groups > More > Mobile Application Settings...**

Table 3-4 *Using the Configure User Mobile Application Settings dialog*

Field, Option, or Button	Information and/or Action
Configure User Mobile Application Settings (*X* users)	
Use default settings	◆ Select this to apply all of the settings in the Configure Mobile Applications dialog to the selected users or groups.
Use user settings to allow mobile applications to:	◆ Select this to apply the settings below to the selected users or groups.
◆ **Access ESN**	◆ Lets selected users/groups access ESN through a ESN mobile app.
◆ **Cache the user's password**	◆ Lets selected user/goups enable the **Save Password** option when logging in to the ESN site through a ESN mobile app.
◆ **Allow files to be added to the Downloads area for offline access**	◆ Lets selected user/groups download files from ESN to mobile devices. ◆ Downloaded files can be viewed in offline mode by accessing the **Downloads** section in the app. ◆ If you don't want users downloading files, make sure that you also disable downloading through web browsers. ◆ Users are responsible for the security of downloaded files. See "Encrypting Downloaded Files" in the "Micro Focus ESN Mobile App 1.0 Quick Start".
◆ **Force PIN Code**	◆ Forces selected user/groups running version 2.0 and later apps to have a 4-digit access code set on their devices for accessing ESN, as described in "Configuring a 4-Digit Passcode" in the "Micro Focus ESN Mobile App 1.0 Quick Start."
◆ **Cut/Copy**	◆ Lets selected user/groups cut or copy data from the ESN mobile app so that the data can be pasted into third-party applications.
◆ **Screen capture (affects Android only)**	◆ Lets selected users/groups take a screen capture while inside the ESN application. **IMPORTANT:** As noted in the option name, this only applies to Android devices. iOS users can always take screen captures.
◆ **Disable applications on rooted or jail-broken devices**	◆ Prevents selected users/groups from running the ESN mobile app on devices that have been rooted or jail-broken.

Field, Option, or Button	Information and/or Action
Open in:	◆ Click the drop-down list and select the option that is best for the selected users or groups as described in the rows below. ◆ Controls whether selected user/sgroups can open files in third-party apps through ESN. For example, a user views a file in ESN, opens and modifies the file in a document editing app, then saves the file back to the ESN app. ◆ iOS calls this "Open In" functionality; Android devices refer to it as "Share" or "Send To." **IMPORTANT:** For MobileIron device management, the following points apply: ◆ In almost all cases the ESN and MobileIron settings must be consistent with each other. ◆ The exception is if you want only the MobileIron-managed devices to have Open In capabilities. To cause this behavior, 1. Enable Open In in MobileIron. 2. Disable Open In in ESN.
◆ **Disabled**	◆ Prevents selected users/groups from opening files in ESN using third-party applications.
◆ **All applications**	◆ Lets selected users/groups open files in ESN using any third-party application.
◆ **Whitelist**	◆ This opens two Whitelists (Android and iOS) of third-party apps that selected users or groups are allowed to open files into. **IMPORTANT** ◆ Only Android package names and iOS bundle IDs are valid list entries. ◆ To get an Android app package name: 1. Install the `Package Name Viewer` app from the Google Play store. This app displays the package name for each app that is currently installed on the device. ◆ To find the bundle ID for an iOS app: 1. Synchronize the app to iTunes from your device. 2. In the iTunes library, open the `Mobile Applications` folder. For iTunes on Mac, the default location is your Home directory at: `~/Music/iTunes/Mobile Applications/` For iTunes On Windows, the default location is `C:\Users\`*username*`\My Music\iTunes\Mobile Applications/` 3. Create a copy of the app's file, and re-save the copy as a `.zip` file. 4. Unzip the newly created `.zip` file. You now see a folder by the name of the application name. 5. Locate the `iTunesMetadata.plist` file within the folder and open it in a text editor. 6. The bundle ID is the string displayed below the `softwareVersionBundleid` key within the file.

Field, Option, or Button	Information and/or Action
OK button	◆ Click this to save your changes. Current user sessions are not affected. To see changes, users must log in to a new session.
Cancel button	◆ Click this to cancel the changes you have made.

Web Browser Access—Default Settings

Path: Port 8443 ESN Admin Console**System > Web Application**

Table 3-5 *Using the Configure Web Application dialog*

Field, Option, or Button	Information and/or Action

◆ **Allow Guest access**	◆ By default, Guest (anonymous) access to ESN is not enabled.
	◆ Selecting this enables anonymous access to ESN through the built-in Guest user account.
	For more information about the Guest and other users, see "Types of ESN Users" in *ESN 1.0: Understanding How ESN Works*.
	IMPORTANT
	    ◆ Guest access is for web users only.
	        Mobile app and desktop users cannot log in as Guest.
	    ◆ Using NetIQ Access Manager to provide single sign-on access as described in the installation guide, prevents Guest user access.

◆ **Guest access is read only**	◆ This is selected by default to prevent Guests from commenting on files or adding files to publicly available folders.
◆ **Disable file downloads**	◆ This is selected by default to prevent all file downloads through web browsers. Individual user or group settings to allow downloads have no effect unless this is deselected.
◆ **Disable web access**	◆ This is selected by default to prevent all users from accessing ESN through a Web browser, unless access is allowed on an individual user or group basis.
OK button	◆ Click this to save your changes. Current user sessions are not affected. To see changes, users must log in to a new session.
Cancel button	◆ Click this to cancel the changes you have made.

Web Browser Access—Individual Users and Groups

Path: Port 8443 ESN Admin Console**Management > Users/Groups >** *select one or more users* **or groups > More >** *select a file download or web access option from the list below*

Table 3-6 *Using the More Options to Control Web Access for Individual Users and Groups*

Field, Option, or Button	Information and/or Action
◆ **Disable File Downloads** ◆ **Enable File Downloads** ◆ **Use Default File Download Setting** ◆ **Disable Web Access** ◆ **Enable Web Access** ◆ **Use Default Web Access Setting**	◆ These options do not all appear at the same time. They change, dynamically, to reflect alternate choices to the options configured in "Web Browser Access—Default Settings" on page 23. ◆ Select an available option in the **More** drop-down list for the selected users or groups. The action is immediately applied to the selected user or group accounts and the drop-down list changes dynamically to reflect the new settings.

4 ESN Clustering Configuration

Path: Port 9443 Appliance Console **Configuration icon > Clustering**

Table 4-1 *Using the Clustering dialog*

Field, Option, or Button	Information and/or Action
Enable Clustered Environment	◆ Click this to enable ESN clustering on this appliance and on all appliances using the same /vashare NFS or CIFS mount point.
◆ **JVM Route**	◆ You can leave this field blank unless you plan to use Apache as the reverse proxy.
	◆ If you plan to use Apache as the reverse proxy, add a JVM route for each ESN Appliance in the Cluster. The purpose of this field is to uniquely identify each ESN Appliance to Apache.
	In the **JVM Route** field, specify `worker1`. On the second ESN node, in the **JVM Route** field, specify `worker2`, and so forth for each ESN node, incrementing the JVM Route setting. Each Tomcat instance should have a unique JVM Route setting.
	`worker1`, `worker2`, and so forth are the default names for the matching values used for the reverse proxy configuration. For example, if you have set up Apache or IIS as a reverse proxy, these are the default values. The **JVM Route** setting in the ESN installer must match these values.
◆ **Hibernate Caching Provider:**	◆ **memcached** is the only option available when configuring ESN in a clustered environment.
	For more information about Memcached caching, see Memcached (http://memcached.org/).
◆ **Server Address:**	◆ The hostnames or IP addresses of both ESNsearch servers, separated by a space.
	◆ After clicking **OK**, you must click **Reconfigure ESN Server** for your changes to take effect.
	This stops and restarts your ESN server. Because this results in server downtime, you should restart the server during off-peak hours.

5 LDAP Servers and Synchronization

LDAP Configuration Dialog

Path: Port 8443 ESN Admin Console**System > LDAP**

Planning Worksheets

Best Practice: Plan your LDAP Servers and use the following worksheets when working in this dialog:

- Worksheet 5 - LDAP Synchronization

Table 5-1   *Using the LDAP Configuration dialog*

Field, Option, or Button	Information and/or Action
LDAP Configuration dialog	
LDAP Servers tab	
◆ **Add** button	◆ Click this to begin the process of adding and LDAP server. The LDAP Server Configuration dialog opens.
◆ **Delete** button	◆ Click this to remove the selected LDAP server from the list. **IMPORTANT:** Before you remove an LDAP server, make sure you consider the options you have set for users and groups that are no longer in LDAP in the *User Settings tab* and the *Group Settings tab*.
◆ **Sync All** button	**TIP:** If you have just added or modified the LDAP Servers configuration, you must save it by clicking **OK** before running an LDAP synchronization. ◆ After your users and groups are synchronized, you can click this to refresh the LDAP information in ESN. ◆ To synchronize only certain users or groups, filter the list by entering a string in the **Filter List**. Or ◆ Click the drop-down arrow next to the Filter List and select the type of users or groups to synchronize. For example, Added users, Modified users, Modified groups, and so forth. ◆ Users and groups that have been modified by running the LDAP sync are reported, along with information about how they have been modified.

Field, Option, or Button	Information and/or Action

◆ **Preview Sync** button	**TIP:** If you have just added or modified the LDAP Servers configuration, you must save it by clicking **OK** before previewing an LDAP synchronization.
	
	◆ Use this to preview the synchronization results—users and groups that will be added or deleted, users that will be disabled, and so on—before you run the actual synchronization.
	
	   ◆ To preview only certain users or groups, filter the list by entering a string in the **Filter List**.
	
	   Or
	
	   ◆ Click the drop-down arrow next to the Filter List and select the type of users or groups to synchronize.
	
	   For example, Added users, Modified users, Modified groups, and so forth.
	
	◆ After you are satisfied with the results, use the **Sync All** option with the same filters to perform the actual synchronization.

◆ **Show Sync Results** button	◆ Use this to display the most recent synchronization results *for the current browser session*. ◆ If you run a synchronization, log out of ESN, and then log in again, no results are available to view.
LDAP servers list	
◆ **Server URL**	◆ The URL you specified when creating the LDAP server. ◆ You can click this to access the LDAP Server Configuration dialog.
◆ **User DN**	◆ This is the LDAP proxy user information for the LDAP server
User Settings tab	
◆ **Register User Profiles Automatically**	◆ Select this option to automatically add LDAP users to the ESN site. ◆ Workspaces are not created until users log in for the first time.
◆ **Synchronize User Profiles**	◆ Select this option to automatically update ESN with user information changes following the initial LDAP synchronization. ◆ The attributes that are synchronized are the attributes listed in the "mappings" box in the *Server Information tab*.
For user accounts provisioned from LDAP that are no longer in LDAP sub-section	
◆ **Disable Account**	◆ This is the default because deleting user accounts cannot be undone. For more information about disabled users in ESN, see Disabling ESN User Accounts in the ESN 1.0: Maintenance Best Practices Guide.
◆ **Delete Account**	**IMPORTANT:** A deleted user cannot be undeleted; this action is not reversible. ◆ Select this only if you have deleted users from your LDAP directory and you want the LDAP synchronization process to also remove them from ESN.
Use the following when creating new users sub-section	
◆ **Time zone:**	◆ Use this drop-down list to set the time zone for user accounts that are synchronized from the LDAP directory into your ESN site. ◆ The time zone list is grouped first by continent or region, optionally by country or state, and lastly by city.

Field, Option, or Button	Information and/or Action
◆ **Locale:**	◆ Use this drop-down list to set the locale for user accounts that are synchronized from the LDAP directory into your ESN site. ◆ The locale list is sorted alphabetically by language.
Group Settings tab	
◆ **Register LDAP group profiles automatically**	◆ Select this to automatically add new LDAP groups to the ESN site.
◆ **Synchronize group profiles**	◆ Select this to synchronize group information, such as the group description, to the ESN site whenever this information changes in LDAP.
◆ **Synchronize group membership**	◆ This option ensures that the ESN group includes the same users (and possibly groups) as the corresponding LDAP group. If this is not selected, then LDAP group changes are not reflected in ESN. ◆ This option also ensures that ESN recognizes group-based file system rights assignment updates. If this is not selected, users with group-based access rights might not qualify for the roles they need to use ESN.
◆ **Delete groups that were provisioned from LDAP but are no longer in LDAP**	**IMPORTANT:** A deleted group cannot be undeleted; this action is not reversible. ◆ Select this only if you have deleted groups from your LDAP directory and you want the LDAP synchronization process to also remove the groups from ESN.
Synchronization Schedule tab	
◆ **Enable schedule**	◆ This is selected by default so that LDAP synchronizations occur at regular intervals. ◆ You should not normally de-select this unless you are troubleshooting a problem or working with Micro Focus support to resolve a service request.
◆ **Every day**	◆ Select this to run an LDAP synchronization every day at the time or interval specified below.
◆ **On selected days**	◆ Select this if you want the LDAP synchronization to run only on specific days.
◆ **At *HH*:*MM***	◆ Using the drop-down lists, you can specify synchronizations to occur at a specific time. ◆ Hours start at midnight (0) and continue through 11 p.m. (23). ◆ Minutes can be specified using 5-minute increments.
Repeat every *X* hours	◆ As an alternative to synchronizing at a specific time, you can set a time interval and synchronize multiple times each day (for example, every four hours). ◆ The smallest time interval you can set is .25 hours (every 15 minutes).
Local User Accounts tab	
◆ **Allow log in for local user accounts (i.e user accounts not in LDAP)**	◆ Use this to enable or disable logging in by locally created and self-provisioned user accounts.

LDAP Server Configuration Dialog

Path: Port 8443 ESN Admin Console**System > LDAP > Add button**

Best Practice: Plan your LDAP Servers and use the following worksheets when working in this dialog:

◆ Worksheet 4 - Users and Groups

Table 5-2 *Using the LDAP Server Configuration dialog*

Field, Option, or Button	Information and/or Action
LDAP Server Configuration dialog	
Server Information tab	
◆ **LDAP Server URL**	**WARNING:** If you modify an existing LDAP connection, do not modify this LDAP server URL field. Doing so can cause synchronized users to be disabled or deleted.
	◆ This is the host name of the LDAP server where your directory service is running.
	Specify a URL with the format your server requires, as follows:
	◆ **Non-SSL:** `ldap://hostname`
	Assumes Port 389 is used
	◆ **SSL:** `ldaps://hostname`
	Assumes Port 636 is used
	This requires that you import the LDAP server's root certificate into the Java keystore before attempting an LDAP synchronization. See "LDAP Synchronization Security" in the *ESN 1.0: Maintenance Best Practices Guide*.
	◆ If the LDAP server uses a different port number from those above, you must include the port as follows:
	◆ `ldap://hostname:port_number`
	◆ `ldaps://hostname:port_number`
◆ **User DN:** (LDAP proxy user)	◆ This is the LDAP proxy user and it must have sufficient rights to access the user information stored there. See "LDAP Proxy User Role and Rights" in *ESN 1.0: Understanding How ESN Works*.
	◆ You must specify a fully qualified, comma-delimited user name, along with its context in your LDAP directory tree, in the format expected by your directory service.
	◆ **eDirectory:**
	`cn=username,ou=organizational_unit,o=organization`
	◆ **Active Directory:**
	`cn=username,ou=organizational_unit,dc=domain_component`

Field, Option, or Button	Information and/or Action
◆ **Password:** (LDAP proxy user password)	◆ You must type the password for the **User DN**.
◆ **Directory Type:**	◆ Select the directory type for the LDAP server that you are configuring (**eDirectory** or **Active Directory**)

◆ **Guid attribute:**	◆ Based on the directory type you have selected, ESN selects the standard LDAP attribute used to identify a user.
	
	◆ **GUID** and **objectGUID:** These are the default, binary attributes for eDirectory and Active Directory, respectively
	
	They have unique values that do not change if you rename or move a user in the LDAP directory, thus ensuring that ESN modifies the existing user rather than creating a new one.
	
	◆ **Other:** Selecting this option in the Guid attribute drop-down prompts you to map users to a different LDAP attribute by specifying the attribute name and then clicking **OK**.
	
	    ◆ You must ensure that the attribute you specify is a binary attribute.
	
	    For example, the cn attribute cannot be used because it is not a binary attribute.
	
	    ◆ If you cancel the prompt to specify an attribute or specify an attribute that is not binary, ESN create new ESN users when names or locations change.
	
	    For example, if you have a ESN user and LDAP user named William Jones, and if William requests that you change his name to Bill in the LDAP directory, then the next time an LDAP synchronization occurs, ESN creates a new user named Bill Jones.

Field, Option, or Button	Information and/or Action

◆ **ESN account name attribute:**	◆ ESN uses this attribute
	
	    ◆ To create ESN account names
	
	    ◆ To locate users in the LDAP directory.
	
	    ◆ As the User ID for authentication purposes.
	
	◆ The value of this attribute must be unique in LDAP.
	
	◆ Attribute options depend on the directory type selected in the **Directory type** drop-down list.
	
	Consult with your directory administrator to determine which attribute or attributes are used in your directory service.
	
	    ◆ For **eDirectory**, the default available options are **cn** and **Other**.
	
	    ◆ For **Active Directory**, the default available options are **sAMAccountName**, **cn**, and **Other**.
	
	    ◆ If you select **Other** as the value for this attribute, you are prompted to enter the name of an LDAP attribute to use instead of the default choices.
	
	◆ Based on your findings, you might need to set up two or more LDAP sources that point to the same LDAP server but use different values for the **LDAP Attribute Used for ESN Name**.
	
	For example, if you use Active Directory, you might need to set up one LDAP source and use cn and another to **sAMAccountName** as the **ESN account name attribute**.
	
	◆ In addition to the attributes already mentioned in this section, other LDAP attributes can be used for the **ESN account name attribute**, as long as the attribute is unique for each User object.
	
	For example, the mail LDAP attribute could be used so that ESN users can log in by using their email addresses.

◆ LDAP Attribute "Mappings" box	◆ This lists the mappings between ESN user information and the LDAP attributes that correspond to them. It is populated automatically. ◆ If Synchronize User Profiles is enabled in the *User Settings tab*, the information associated with the mappings that are configured here, is updated each time the user account is synchronized.
OK button	◆ If you are modifying previously configured LDAP server information, you can click **OK**. Otherwise, you must click the *Users tab*
Cancel button	◆ Click this to discard the LDAP server configuration changes you have made and exit the tab.
Users tab	
◆ **Add** button	◆ Click this to open the "LDAP Search Dialog (User Version)" on page 33 wherein you can specify a context where ESN searches for LDAP users.
◆ **Delete** button	◆ Click this after selecting one or more list entries. For example, when the context no longer exists or when it is covered by another entry.

Field, Option, or Button	Information and/or Action
OK button	◆ If you are modifying previously configured User information, you can click **OK**. ◆ If this is a new configuration, you should click the *Groups tab* and add an LDAP search context. Otherwise, your ESN users might not be recognized as having the roles needed for ESN access (see the information for the "Synchronize group membership" option).
Cancel button	◆ Click this to discard your changes and exit.
Groups tab	
◆ **Add** button	◆ Click this to open the LDAP Search Dialog (Group Version) wherein you can specify a context where ESN searches for LDAP groups.
◆ **Delete** button	◆ Click this after selecting one or more group Base DN entries. For example, when the context no longer exists or when it is covered by another entry.
OK button	◆ Click **OK** to save the LDAP server configuration.
Cancel button	◆ Click this to discard your changes and exit.

LDAP Search Dialog (User Version)

Path: Port 8443 ESN Admin Console**System > LDAP > Add button > Users tab > Add button**

Table 5-3   Using the LDAP Search dialog (User Version)

Field, Option, or Button	Information and/or Action
✓ **LDAP Search dialog (User Version)**	

◆ **Base DN:**	**Best Practice:** Use the **Browse** icon [⬚] next to the **Base DN** field to browse the LDAP directory for the base DN that you want to use. This eliminates the risk of typing the context incorrectly. Also, if browsing fails, that means the LDAP server configuration is not correct and must be changed.
	
	◆ This is the directory context or container under which LDAP User objects are located.
	
	◆ When specifying this you must use the syntax required by your directory service type.
	
	  ◆ **eDirectory:** `ou=organizational_unit,o=organization`
	
	  ◆ **Active Directory:**
	  `ou=organizational_unit,dc=domain_component`
	
	IMPORTANT: Container names cannot exceed 128 characters. If they do, users are not provisioned.

Field, Option, or Button	Information and/or Action
◆ **Filter:**	◆ **IMPORTANT:** ESN sets up a standard user filter for the LDAP server type.
	In almost all cases, this doesn't require modification.
	◆ **About User Filters:**
	◆ By default, ESN identifies potential users by filtering on the following LDAP directory object attributes:
	◆ `Person`
	◆ `orgPerson`
	◆ `inetOrgPerson`
	If needed, you can modify the filter by inserting the following operators:
	◆ | OR (the default)
	◆ & AND
	◆ ! NOT
	◆ **A Group for ESN Users:**
	◆ You might want to create a group for only ESN users, regardless of where they are located in your LDAP directory.
	◆ After creating the group, use the following filters to search for User objects that have the group membership attribute shown below.
	Make sure you include the parentheses in your filter.
	◆ **eDirectory:**
	`(groupMembership=cn=`*`group_name`*`,ou=`*`organizational_unit`*`,o=`*`organization`*`)`
	◆ **Active Directory:**
	`(memberOf=cn=`*`group_name`*`,ou=`*`organizational_unit`*`,dc=`*`domain_component`*`)`
	IMPORTANT: Users in eDirectory sub-groups are not synchronized.
	However, for Active Directory you can create a filter that synchronizes users in sub-groups by using the following rule object identifier (OID):
	`<attribute name>:<matching rule OID>:=<value>`
◆ **Search subtree**	◆ Select this if you want ESN to search for users in containers underneath the base DN (that is, in subtrees).

LDAP Search Dialog (Group Version)

Path: Port 8443 ESN Admin Console**System > LDAP > Add button > Groups > Add button**

Table 5-4 *Using the LDAP Search dialog (Group Version)*

Field, Option, or Button	Information and/or Action
🖊 **LDAP Search dialog (Group Version)**	

Field, Option, or Button	Information and/or Action

◆ **Base DN:**	**Best Practice:** Use the **Browse** icon ⬚ next to the **Base DN** field to browse the LDAP directory for the base DN that you want to use. This eliminates the risk of typing the context incorrectly. Also, if browsing fails, that means the LDAP server configuration is not correct and must be changed.
	
	◆ This is the directory context or container under which LDAP Group objects are located.
	
	◆ When specifying this you must use the syntax required by your directory service type.
	
	    ◆ **eDirectory:** ou=*organizational_unit*,o=*organization*
	
	    ◆ **Active Directory:**
	    ou=*organizational_unit*,dc=*domain_component*
	
	IMPORTANT: Container names cannot exceed 128 characters. If they do, groups are not provisioned.

◆ **Filter:**	◆ **IMPORTANT:** ESN sets up a standard group filter for the LDAP server type. In almost all cases, this doesn't require modification.
◆ **Search subtree**	◆ Select this if you want ESN to search for groups in containers underneath the base DN (that is, in subtrees).

6 Licensing

Installing/Updating the ESN License

IMPORTANT: If you have an expandable deployment, you must update the license on each ESN appliance in the cluster.

PostgreSQL and ESNsearch appliances do not require licenses.

Path: Port 9443 Appliance Console **Configuration icon > License**

Table 6-1 *Using the License (port 9443) dialog*

Field, Option, or Button	Information and/or Action
◆ **Choose File** button	1. Download your `license-key.xml` file (from the Novell Customer Center (NCC)) to your management workstation. 2. Click **Choose File**. 3. Browse to and select the downloaded license file. 4. Click **Open**. 5. Click **Reconfigure ESN Server** in the **Configuration** column.

Viewing ESN License Details

Path: Port 8443 ESN Admin Console **> Management > License**

Table 6-2 *Using the License (port 8443) dialog*

Field, Option, or Button	Information and/or Action
◆ **Current License**	This section displays information about the installed license, including: ◆ Information about the license key, when it was issued, and who issued it. ◆ Product and version information. ◆ The effective date range. ◆ Information about user allowances. Your contract contains details. Internal users might or might not be restricted; external (ESN administrator-created) users are not restricted. ◆ The options or features that the license enables for use.

Field, Option, or Button	Information and/or Action
◆ **Reload License File**	◆ If the license information displayed doesn't seem correct, click this to reload the file and refresh the display.
	◆ If you need to install a new license file, see "Installing/Updating the ESN License" on page 37.

7 Logging and Monitoring

Accessing ESN System Log Files

Path: Port 9443 Appliance Console**System Services icon**

Table 7-1 *List of System Log Files*

Field, Option, or Button	Information and/or Action

• **Log Files column**	• Click one of the **Download** links to download the log files for the following services.
	
	   • **Novell ESN:** `catalina.out`, `appserver.log`
	     The `catalina.out` file reports all timestamps in UTC/GMT.
	     (ESN appliance)
	
	   • **Jetty:** `jetty.stderrout.log`
	     (ESN, ESNsearch, and PostgreSQL database appliances)
	
	   • **Postfix:** `mail`
	     (ESN appliance)
	
	   • **Novell FAMT:** `famtd.log`
	     (ESN appliance)
	
	   • **Search:** `indexserver.log`
	     (ESNsearch appliance)
	
	   • **PostgreSQL:** `PostgreSQLd.log`
	     (PostgreSQL appliance)
	
	   • **Memcached:** `jetty.stderrout.out`
	     (ESNsearch appliance)

Automatically Applying Deferred Search Logs

Path: Port 8443 Appliance Console **Search Index > Update Logs**

Table 7-2 *The Configure Update Logs dialog*

Field, Option, or Button	Information and/or Action
◆ **Automatically Apply Deferred Update Logs in Background**	**IMPORTANT** ◆ The application of update logs is integral to ESN system design and data integrity. ◆ You should never disable this option unless instructed to do so by a support technician as part of resolving an incident report.

Changing the Ganglia Monitoring Configuration

Ganglia is a scalable, distributed monitoring system that lets you gather important information about your ESN system.

Path: Port 9443 Appliance Console**Ganglia Configuration icon**

Table 7-3 *Using the Ganglia Monitoring Configuration dialog*

Field, Option, or Button	Information and/or Action
Monitoring Services	
Enable Full Monitoring Services	◆ Deselect this if: 　◆ You already have a monitoring system that you plan to use for ESN. 　◆ You plan to configure a dedicated appliance for viewing monitoring information. 　You do this by selecting **Unicast** below and then specifying the DNS name or IP address of the appliance where monitoring information will be collected. ◆ (Default) Select this to have this appliance receive and store metrics from other appliances, and to allow the Ganglia Web Interface to run on the same machine as the ESN appliance.
Monitoring Options	
Enable Monitoring on this appliance	◆ (Default) Select this option to enable Ganglia monitoring on this appliance.
◆ **Multicast**	◆ (Default) Send performance data to the other appliances on the network (default setting).
◆ **Unicast**	◆ Send monitoring information to a single destination. This is a best practice recommendation for performance.
◆ **Publish to:**	◆ The URL where you want Ganglia to send monitoring information when it is running in Unicast mode.
Monitoring Tool Options	
◆ **Enable direct http port 9080 access**	◆ Select this to allow Ganglia to communicate using HTTP port 9080.

Field, Option, or Button	Information and/or Action
◆ **Reset Database** button	◆ Click this to remove all existing Ganglia metrics from this appliance. This option is not related to the ESN database.

See Also

- ◆ "Monitoring" in the *ESN 1.0: Maintenance Best Practices Guide*.
- ◆ The Ganglia Monitoring System web site (http://ganglia.info/).

Generating ESN-Monitoring Reports

Path: Port 8443 ESN Admin Console**System > Reports**

Table 7-4 Using the Reports dialog

Field, Option, or Button	Information and/or Action
About the Reports	◆ Most reports are created in CSV format for importing into a spreadsheet and manipulating the data to suit your needs. A few reports are displayed in the Reports window. ◆ The default file name for CSV-format reports is `report.csv`. If you create multiple reports without manually renaming them, the default file name is incremented—`report (n).csv`. ◆ CSV-format reports are saved in the default download directory for the browser being used.
◆ **Run a Report:**	◆ Click the drop-down list and select a report to run. The following sections describe the contents of each report.

- ◆ "Credits Report" on page 41
- ◆ "Email Report" on page 42
- ◆ "External User Report" on page 42
- ◆ "License Report" on page 42
- ◆ "Login Report" on page 43
- ◆ "System Error Logs Report" on page 43
- ◆ "User Access Report" on page 43
- ◆ "User Activity Report" on page 44
- ◆ "XSS (Cross-Site Scripting) Report" on page 45

Credits Report

Path: Port 8443 ESN Admin Console**System > Reports > Run a Report: > Credits**

This report displays the portions of ESN that are subject to third-party copyrights and licenses.

Email Report

Path: Port 8443 ESN Admin Console**System > Reports > Run a Report: > Email Report**

- *Date Range***:** The date range defaults to the past month, but dates can be set by clicking in the date fields and using drop-down widgets to change the range.
- **Sent emails:** Information about sent emails displays in the **Reports** window.
- **Error emails:** Information about email-associated errors displays in the **Reports** window.
- **Received emails:** Not operational because ESN cannot receive emails.
- Displayed reports include the following information:
  - **Send Date:** When the email was sent.
  - **From Address:** Address that the email was sent from.

    This is the email address defined in the user profile.
  - **To Address:** Address that the email was sent to.
  - **Type:** Action that caused the message to be sent.

    For example, `sendMail` indicates that an item was shared.
  - **Status:** Status of the message.
  - **Subject Line:** Subject line of the message.
  - **Attached Files:** File name of any attachments that were included in the email message.
  - **Errors:** Any errors associated with the email message.

External User Report

Path: Port 8443 ESN Admin Console**System > Reports > Run a Report: > External User Report**

- Lists information about the external users you include in the **People** field.

  If the **People** field is left blank, all external users are included.

License Report

Path: Port 8443 ESN Admin Console**System > Reports > Run a Report: > License Report**

The License report lists the following information in the Reports window:

- ESN version (**ProductTitle**)
- License key type (**Key uid**)
- Date the license key was issued (**Key issued**)
- Date range when the license key is valid (**Effective**)
- Information regarding registered and external user allowances.
- The *Date Range* covered by the report (as set before **Create Report** is clicked)
- **Current Active User Count**—user accounts that are not disabled.
- List of dates in the date range with the following user license information:
  - **Date:** The date for which the data in the row applies.
  - **Local Users:** User accounts created within ESN and not being synchronized from an LDAP directory.

- **Users Synchronized from LDAP:** User accounts created from an LDAP source. (Only synchronized accounts that are not marked as Deleted or Disabled are counted.)
- **Users with OpenID Accounts:** OpenID is no longer supported. Users that self-provisioned using an OpenID account.
- **Self Registered Users:** User accounts created when users self-provisioned.
- **Guest Access Enabled:** Whether Guest access was enabled on the listed date.
- **Users in the Past 365 Days:** Users who have logged in at least once in the past year.
- **Checksum:** <waiting for information from Sanjeev.>

Login Report

Path: Port 8443 ESN Admin ConsoleSystem > Reports > Run a Report: > Login Report

---

NOTE: This report only covers web client users. Mobile and Desktop users are not currently tracked.

- *Date Range:* The date range defaults to the past month, but dates can be set by clicking in the date fields and using drop-down widgets to change the range.
- **People:** All users are covered by default, but you can begin typing names and use the name-completion widget to select specific users for the report.
- **Summarize Login Entries:** Summarizes how many times the selected users have logged in using a web browser.

  The **Sort Report By** drop-down list, lets you presort the data alphanumerically by **User**, **Last Login**, or **Number of Logins**.
- **List All Login Entries:** Lists each successful log in to the web client and includes the following data about the action:
  - User (first name, last name, and user ID)
  - Account type
  - Login date and time
  - IP address

  The **Sort report by** drop-down list lets you presort the data alphanumerically by either **Login Date** or **User**.

System Error Logs Report

Path: Port 8443 ESN Admin ConsoleSystem > Reports > Run a Report: > System Error Logs

Use this to download a `logfiles.zip` file of the error logs currently on the system.

- **Download Log:** Generates a logfiles.zip file that contains the error logs currently on the system.
  - The zip file is downloaded to the browser's download directory.
  - If you download multiple zip files without manually renaming them, the file name is incremented—logfiles (*n*).zip

User Access Report

Path: Port 8443 ESN Admin ConsoleSystem > Reports > Run a Report: > User Access Report

This report shows each ESN location that the specified user has access to.

- **User:** Use the name-completion widget (type then select a name) to select a user you want to check.

  A report for the user is automatically displayed in the Reports window, showing each location that the user has access to.

User Activity Report

Path: Port 8443 ESN Admin Console**System > Reports > Run a Report: > User Activity Report**

This report summarizes the significant actions that specified users have taken on the ESN site during a specified period of time.

- *Date Range***:** The date range defaults to the past month, but dates can be set by clicking in the date fields and using drop-down widgets to change the range.
- **People:** All users are covered by default, but you can begin typing names and use the name-completion widget to select specific users for the report.
- **Activity Summary:** This report lists how many times the selected users have performed the following actions in the ESN site:
  - User reported on
  - Views
  - Adds
  - Edits
  - Renames
  - Deletes (purge)
  - Pre-Delete (delete but not purge)
  - Restores (restore a deleted item that has not been purged)
  - ACL changes
  - Add shares
  - Modify shares
  - Delete shares
- **Workspace or Folder Activity:** This report lists each individual user action and includes the following data about the action:
  - User performing the action
  - Activity type
  - Count
  - Activity date and time
  - Folder
  - Entry title
  - Entity type
  - Share Recipient
  - Recipient Type
  - Share Role

XSS (Cross-Site Scripting) Report

Cross-site scripting (XSS) is a client-side computer attack that is aimed at web applications. Because XSS attacks can pose a major security threat, Micro Focus ESN contains a built-in security filter that protects against XSS vulnerabilities. For more general information about XSS, see "XSS—ESN Is Secure" in the *ESN 1.0: Maintenance Best Practices Guide*.

Path: Port 8443 ESN Admin Console**System > Reports > Run a Report: > User Activity Report**

- ◆ **Select the binders to be checked:** Navigate the directory structure and select the directories you want to scan, then click **Create Report**.

  The generated lets you to remove potentially harmful XSS threats from your ESN site.

IMPORTANT: Because XSS attacks often are designed to wait for users with extra privileges (such as the administrator) to view the page where the attack was set, it is important that you don't navigate to the page after you run the report.

For information about how to run the XSS report and safely remove XSS threats, see "TID 7007381: Running the XSS Report in Micro Focus ESN" in the Novell Support Knowledgebase (http://www.novell.com/support).

Logging All HTTPS Traffic

Path: Port 9443 Appliance Console **Configuration icon > Logging**

Table 7-5 *Using the Logging dialog*

Field, Option, or Button	Information and/or Action
◆ **Enable host access logging**	◆ Selecting this generates a single file that contains log information for all HTTPS traffic and can become large very quickly.
	◆ If the file grows too large, you must disable this option.
	NOTE: By default, non-https logging is always enabled on the appliance. (For information about how to access the ESN log file, see "System Error Logs Report" on page 43.)

Managing Audit Trail Logs of Database Activity

Path: Port 8443 ESN Admin Console**Management > Database Logs**

Table 7-6 *Using the Manage Database Logs dialog*

Field, Option, or Button	Information and/or Action

Automatically Delete Audit Trail Entries Older Than *X* Days	◆ This defines the maximum number of days to keep audit trail log entries before they are deleted.
	
	The default is 183 days (6 months).
	
	The allowed minimum is 30 days.
	
	IMPORTANT: Before changing this, consider the following:
	
	  ◆ Audit trail entries are used to build the Activity and Login reports. Removing older entries limits the time span that these reports can cover. (For more information about these reports, see "Generating ESN-Monitoring Reports" on page 41.)
	
	  ◆ The ESN desktop application relies on audit trail data when doing full synchronizations.

8 Network Infrastructure

- ["Changing Network Settings" on page 47](#)
- ["Network Configuration" on page 48](#)
- ["Port Numbers" on page 49](#)

Changing Network Settings

The settings in this dialog are set during initial deployment.

Path: Port 9443 Appliance Console**Network icon**
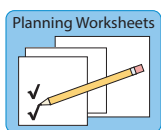
Best Practice: Be sure to update your record:

- Worksheet 20 - Network Support

Table 8-1 *Using the Network (DNS, IP, Access restrictions) dialog*

Field, Option, or Button	Information and/or Action
Network (IP Infrastructure) dialog	Worksheet 20 - Network Support (IP Address Infrastructure Information and Appliance-Specific IP Configuration Settings)
DNS Configuration section	
• **Name Servers:**	• You can modify the name servers.
• **Search Domains:**	• If this field is left blank, it is auto-populated with the domain of the appliance hostname. For example, if the hostname of the appliance is `ESN.mycompany.com`, the domain is auto-populated with `mycompany.com`.
• **Gateway:**	• Make sure that this matches any of the other changes you have made in this dialog.

NIC Configuration section	• In this section, you can modify the IP address, hostname, and network mask of any Network Interface Controller (NIC) associated with the appliance. (If you configured multiple NICs for the ESN appliance, you can configure the additional NICs.)
	
	  • In the **NIC Configuration** section, click the ID of the NIC.
	
	  • Edit the IP address, hostname, or network mask.
	
	    If you change the IP address, you must restart the appliance in order for the change to be reflected.
	
	  • Click **OK**.

Field, Option, or Button	Information and/or Action
Appliance Administration UI (Port 9443) Access Restrictions section	◆ In this section, specify the IP address of any networks for which you want to allow access to the ESN site. ◆ Leave this section blank to allow administrative access from any network.
OK button	◆ Click this to save your changes, then click **Reconfigure ESN Server**. This stops and restarts your ESN server. Because this results in server downtime, you should restart the server during off-peak hours. User sessions can be affected by the above changes.
Cancel button	◆ Click this to cancel the changes you have made.

Network Configuration

Path: Port 9443 Appliance Console > **Configuration icon > Network**
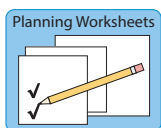
Best Practice: Plan your network infrastructure in advance and use the following worksheet when working in this dialog:

◆ Worksheet 20 - Network Support

Table 8-2   Using the Network (Port Redirection) dialog

Field, Option, or Button	Information and/or Action
Network (Communication Configuration) dialog	Worksheet 20 - Network Support (Network Communication Configuration)
◆ **Port Redirection**	◆ Select this option to have ESN automatically redirect from ports 80 or 443 (which are the standard ports for Web browsers) to ports 8080 and 8443 (which are the default ports that ESN listens on). Enabling port redirection in this way allows users to specify the ESN site URL without including the port number. If port redirection is not enabled, users must include the port number in the site URL when accessing the ESN site. **IMPORTANT:** When port redirection is enabled, ensure that the reverse proxy ports are set to 80 for the HTTP port and to 443 for the secure HTTP port. If they are not, URLs that are sent with ESN email notifications will continue to have the default port (8443) in them. For information about how to change the reverse proxy ports, see <Reverse Proxy Configuration Settings [hidden as Preview profile]>.

Field, Option, or Button	Information and/or Action
◆ **HTTP Port:**	◆ The default HTTP port is 8080. As a best practice, do not change this from the default port. ◆ Select **Enabled** if you want to enable the HTTP port. By default, only the Secure HTTP port is enabled. ◆ Select **Force Secure Connection** to force users to connect to ESN over a secure connection (HTTPS). See "Port Numbers" on page 49 for more information about port numbers in ESN.
◆ **HTTPS Port:**	◆ **HTTPS Port:** The default secure HTTP port for ESN is 8443. As a best practice, do not change this from the default. See "Port Numbers" on page 49 for more information about port numbers in ESN.
◆ **AJP Port:**	◆ For an explanation of the Apache JServ Protocol port, see *The AJP Connector* (http://tomcat.apache.org/tomcat-6.0-doc/config/ajp.html).
◆ **Session Timeout**	◆ By default, if a user's Micro Focus ESN session is idle for four hours (240 minutes), ESN logs the idle user out. For increased convenience to ESN users, you can make the session timeout interval longer. For increased security for your ESN site, you can make the session timeout shorter.
◆ **Forward Proxy Host Name**	No longer used.
◆ **Forward Proxy Port**	No longer used.
OK button	◆ Click this to save your changes, then click **Reconfigure ESN Server**. This stops and restarts your ESN server. Because this results in server downtime, you should restart the server during off-peak hours. Current user sessions are not affected. To see changes, users must log in to a new session.
Cancel button	◆ Click this to cancel the changes you have made.

Port Numbers

Table 8-3 lists the ports that you need to take into consideration when setting up ESN. Figure 8-1 is a graphical representation of how some of the ports are used in a ESN deployment.

As a best practice, do not change any port numbers from the default ports.

Table 8-3   *ESN Port Numbers*

Port Numbers	Description
80, 443	Standard Web server ports

Port Numbers	Description
8080, 8443	Default Tomcat ports for the ESN appliance
	When you install ESN, Tomcat is installed along with the ESN software. ESN uses Tomcat as a stand-alone web server for delivering data to ESN users in their web browsers. For more information about Tomcat, see the Apache Tomcat Web site (http://tomcat.apache.org).
9090, 9443	Jetty port for the appliance (Administrator Interface)
9080	Apache/HTTPD port
8005	Default shutdown port
	For an explanation of the shutdown port, see *Tomcat - Shutdown Port* (http://www.wellho.net/mouth/837_Tomcat-Shutdown-port.html).
8009	Default AJP port
	For an explanation of the Apache JServ Protocol port, see *The AJP Connector* (http://tomcat.apache.org/tomcat-6.0-doc/config/ajp.html).
22	SSH port for the appliance
111	rpcbind utility
1099	Java RMI port
4330	FAMT port
7380, 7443	Ganglia RRD-REST ports
8380, 8381	Default Jetty ports
8642, 8649, 8650, 8651, 8652	Ganglia web interface port
1199	Lucene RMI registry port
1188	Lucene server port
3306	PostgreSQL outbound port
1433	Microsoft SQL server port
25, 465	SMTP and SMTPS outbound ports
6901	OES DFS JetStream port
524/tcp	Access OES server over NCP
137/tcp, 137/udp, 138/udp, 139/tcp, 445/tcp	Access servers over CIFS
88	Kerberos port
11211	Used for memcached caching in an appliance cluster
636	Secure LDAP port
389	Non-secure LDAP port

Figure 8-1 *ESN Port Usage*

Port(s)	Destination
524, 389/636, 6901	NetWare
136, 137, 138, 139, 445, 389/636, 88	Windows / OES
445	CIFS Storage
111, 2049	NFS Storage
25, (465/587)	Mail
22, 3306, 8649, 9443	MySQL
22, 1188, 1199, 8649, 9443, 11211	Filrsearch

Personal Devices, Workstations, Browsers — 80, 443 — L4 Switch — 22, 8443, 9443 — Filr

Protocol Key

▶ REST   ▶ NCP   ▶ CIFS   ▶ NFS   ▶ System Protocols
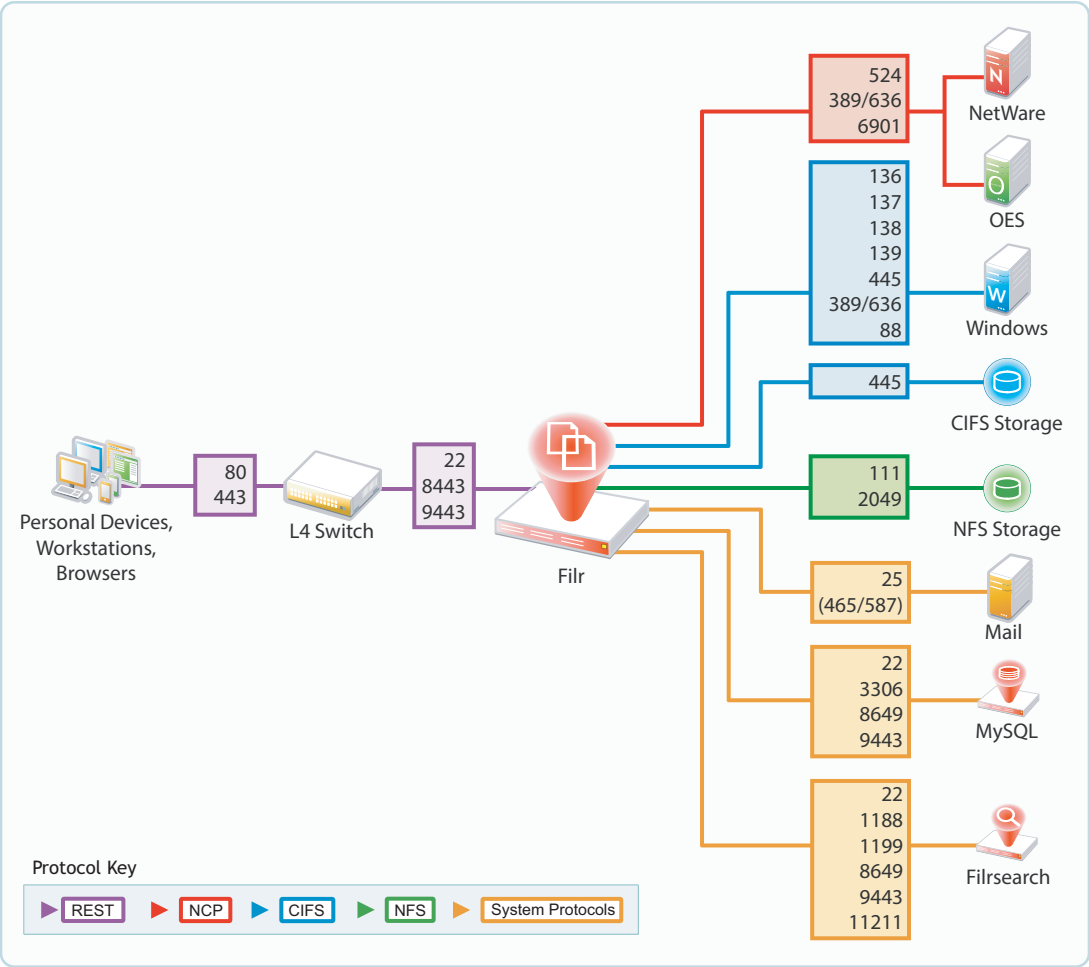
9 Notifications (Email)

ESN can send notifications through email about what is happening on the system. For an overview of ESN's notification services, see "ESN Email Notifications" in *ESN 1.0: Understanding How ESN Works*

To configure ESN's notification services, see the following sections:

- "Configuring an Email Service for ESN to Use" on page 53
- "Enabling Notifications" on page 55

Configuring an Email Service for ESN to Use

Path: Port 9443 Appliance Console **Configuration icon > Outbound E-Mail**

TIP

- If you make changes in this dialog, you must select **Reconfigure ESN Server** for them to take effect.

  Because reconfiguring ESN causes a system restart, you should only change these settings during off-peak hours.

Planning Worksheets

√
√

Best Practice: Plan the email service that will handle outgoing notifications in advance and use the following worksheet when working in this dialog:

- Worksheet 13 - Notifications

Table 9-1   *Outbound Email dialog*

Field, Option, or Button	Notes
Outbound Email dialog	
◆ **Use Local Postfix Mail Server**	By default, ESN is configured with an active Postfix mail server system. ◆ To use another mail system (such as GroupWise), deselect this option, then specify the appropriate information for the system that ESN will use instead.

Field, Option, or Button	Notes
◆ **Protocol:**	◆ Specify whether the email system that ESN will leverage uses SMTP or SMTPS (secure SMTP). For GroupWise, check how the Internet Agent is configured. ◆ If the email system requires SMTPS, see "Email Transfer Security" in the *ESN 1.0: Maintenance Best Practices Guide*.
◆ **Host:**	◆ Specify the host name of the mail server that ESN will leverage. If you are using GroupWise, this is the host name of a server where the Internet Agent is running.
◆ **Port:**	◆ Specify the port through which ESN can connect to the SMTP mail server. GroupWise always uses port 25, even when SSL is enabled. Some mail servers require port 465 or 587 for SMTPS connections.
◆ **Time zone:**	◆ You can change the time zone if you want ESN to use an email time stamp that is different from the time zone where the server is located. The time zone list is grouped first by continent or region, optionally by country or state, and lastly by city.
◆ **User Name:**	◆ Specify the email address that ESN will use when sending emails. If the email server requires authentication, ESN sends this username. Many SMTP mail hosts require a valid email address before they establish the SMTP connection. Although some email systems can construct a valid email address if you specify only a valid user name, you should provide a valid email address to ensure a successful connection. Email notifications from ESN will show this email address in the **From** field.
◆ **Password:**	◆ If the email server requires passwords, specify the password for the user name.
◆ **Authentication Required**	◆ If the email server ESN is leveraging requires authentication, select this option. **GroupWise** The GroupWise Internet Agent does not require authentication for inbound messages. However, the /forceinboundauth startup switch in `gwia.cfg` will cause the Internet Agent to refuse SMTP connections unless a valid email user name and password are provided. The Internet Agent can accept just the user name or the full email address. **Exchange** If you set up the outbound email server to require authentication (by selecting the option **Authentication Required**), Exchange must be configured to allow the From address to be different from the user who is configured for Exchange authentication. The Exchange permission that you need to add is `ms-Exch-SMTP-Accept-Any-Sender.` This is needed because Exchange, by default, requires that the From address of outbound emails match the exchange user who is configured for authentication, and many ESN emails place the email address of the user performing an action in the From field.

Field, Option, or Button	Notes
◆ **Allow sending e-mail to all users**	◆ If you select this option, users can send email to the All Users group. This is disabled by default because of the potential for users to send large numbers of emails.
◆ **Force HTTPS links**	◆ Select this if all links in ESN-generated email messages should be HTTPS instead of HTTP. Otherwise, ESN uses its connection (HTTP or HTTPS) with the emailing user as the link protocol.
◆ **Enable STARTTLS**	◆ Select this option if the email service that ESN is leveraging requires TLS over SMTP for secure email.
◆ **From e-mail address override:**	◆ If you don't want the **User Name** email address used in the **From** field in ESN messages, specify a different address here.
◆ **Use from e-mail address override for all outbound e-mail**	◆ Select this option to have ESN always use the **From email address override** email address in system-generated emails (summarized in "Enabling Notifications" on page 55). If this option is not selected, the **From email address override field** is used only in digest subscription emails.
◆ **Connection Timeout:**	◆ Specify the amount of time for ESN to wait before timing out on a connection request to the email host.
◆ **Test Connection**	◆ Click this to test your Outbound E-Mail configuration.

Enabling Notifications

Path: Port 8443 ESN Admin Console **> System > Email**

By default, ESN users can have the ESN system send email notifications when they create folders, add files, share files and folders, and so on.

Planning Worksheets
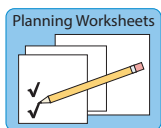
Best Practice: Plan for whether ESN will generate email notifications, how often they will be sent, and how large associated attachments can be and use the following worksheet when working in this dialog:

◆ Worksheet 13 - Notifications

Table 9-2 *Using the Email dialog*

Field, Option, or Button	Notes
✓ **Email** dialog	

Field, Option, or Button	Notes
◆ **Enable Outgoing Email**	◆ Use this option to control whether the ESN system generates email notifications. If you de-select this option, no notifications are sent. This option has no effect on the ability for ESN users to email each other.
◆ **Default Digest Schedule**	◆ Use this section to schedule how often ESN sends activity digests to subscribers. For information about users subscribing to receive ESN activity digests, see "Subscribing to a Folder or File" in the *ESN 1.0: User Access Guide*). For information about users subscribing other users to receive digest for folders that they share, see "Configuring Folders to Send Email Notifications to Other Users" in the *ESN 1.0: User Access Guide*).

◆ **Outgoing Email Quotas**	◆ When users subscribe themselves or others to receive email notifications, there is an option to have the email include changed or new files as attachments.
	
	Use the options in this section to control the size of email attachments, as follows:
	
	  ◆ To preserve the default of no size restrictions, leave the fields blank.
	  ◆ To limit attachment sizes, specify the maximum amounts for either or both fields.
	  ◆ To prevent any attachments from being sent, specify 0 (zero) in each field.

10 Performance Tuning

See also *Tuning ESN 1.0 for Performance*

Changing Configuration Settings for Requests and Connections

Configure the number of client requests and database connections that ESN supports.

Path: Port 9443 Appliance Console **Configuration > Requests and Connections**

Table 10-1 Using the Requests and Connections dialog

Field, Option, or Button	Information and/or Action
Requests and Connections	◆ **Max Threads:** The maximum number of simultaneous client request threads that ESN will support. Default: 250 ◆ **Max Active:** The maximum number of database connections that can be allocated simultaneously from this pool. Default: 300 ◆ **Max Idle:** The maximum number of database connections that can be simultaneously idle in this pool. Default: 300 ◆ **Scheduler Threads:** The size of the thread pool used for background execution of scheduled tasks. Default: 20 ◆ **Max REST Requests (upload/download):** The maximum number of concurrent desktop and mobile, upload and download requests that ESN will handle simultaneously. Default: 50 Ensures that ESN does not exceed capacity. Excess requests are cached so that ESN can respond when it has bandwidth.
OK button	◆ After clicking this, you must click **Reconfigure ESN Server** for the changes to take effect.

TIP: Extremely large ESN sites requesting numerous client requests and database connections might see improved performance by increasing these settings.

Changing JVM Configuration Settings

Path: Port 9443 Appliance ConsoleConfiguration icon > JVM Settings

Table 10-2   *Using the JVM Settings dialog*

Field, Option, or Button	Information and/or Action
JVM Settings	**Best practice recommendation:** Set both sizes to 66% of total RAM (see "Appliance Memory and CPU" in the ESN 1.0: Installation, Deployment, and Upgrade Guide).
	Although ESN can begin with the minimum and adjust up to the maximum as needed, the adjustment process is resource intensive and degrades system performance.
	IMPORTANT: Values must end with g or m and cannot contain fractional values. For example, to set the JVM min heap size to 1.5 GB, specify 1536m.
	◆ **JVM Min Heap Size:** Increase or decrease as needed.
	Default: 6g
	◆ **JVM Max Heap Size:** Increase or decrease as needed.
	Default: 6g
	◆ **Java Home:** Informational only; cannot be changed.
	◆ **Allow generation of a system dump on a user signal:** Causes generation of a system dump in addition to a heap dump and java core dump at the time a dump is triggered on a user signal.
	This can be useful when troubleshooting issues with your ESN system. However, a system dump takes more time and the files consume more disk space than a heap dump or java core dump.
OK button	◆ After clicking this, you must click **Reconfigure ESN Server** for the changes to take effect.

11 Personal Storage

Enabling Personal Storage for Users and Groups

Path: Port 8443 ESN Admin Console Management > Personal Storage > Allow LDAP Users to Have Personal Storage Area

 Best Practice: Plan for whether ESN users can have files and folders stored directly on the ESN appliances' shared storage disk:

- Worksheet 11 - Personal Storage

Table 11-1   Using the Personal Storage (enable) dialog

Field, Option, or Button	Information and/or Action
Personal Storage dialog	Worksheet 11 - Personal Storage (Enabling Personal Storage)
• **Allow LDAP users to have personal storage area**	• Select or deselect this, depending on whether you want all users whose accounts are synchronized via LDAP to have access to personal storage in the My Files area. To learn more about personal storage, see My Files (Personal Storage) in the ESN 1.0: Understanding How ESN Works. **IMPORTANT:** This lets you enable personal storage for all users. Unlike some other configuration options, it is not required for personal storage to be available. Personal storage can also be enabled or disabled on a user or group basis irrespective of this setting. • **Individual Users:** To enable or disable personal storage for individual users, see Table 22-1, "Using the Users dialog," on page 99. • **Groups of Users:** To enable or disable personal storage for groups of users, see Table 22-3, "Using the Groups dialog," on page 102.

Managing and Restricting ESN-Based Storage

Disk space usage almost always increases over time. You can limit on the amount of data that can be uploaded to ESN's shared storage disk at the system level or for individual users and groups.

Only files count toward the data quota. Empty folders don't count. Files in Net Folders don't count.

You can limit the amount of disk space for individual users and groups as well as for individual folders.

Path: Port 8443 ESN Admin ConsoleManagement > Personal Storage

Best Practice: Plan whether personal storage disk space restrictions are required and implement your plans here.

 ◆ Worksheet 11 - Personal Storage

IMPORTANT: Data quotas at all levels are strictly enforced. If uploading a file would cause a user to exceed the assigned quota, ESN rejects the upload attempt and the attempt is aborted. This is also true with data quotas that are set on folders.

Table 11-2   *Using the Personal Storage (data quota) dialog*

Field, Option, or Button	Information and/or Action
Enable User Data Quotas section	Worksheet 11 - Personal Storage (Enable User Data Quotas section)

◆ **Enable User Data Quotas**	**NOTE:** Data quotas only apply to personal storage.
	
	 Enabling Data Quota Enforcement
	
	 ◆ Select this to enable
	      ◆ Enforcement of the default data quota for all unlisted users and groups
	      And
	      ◆ Enforcement of the data quotas shown for the listed users and groups
	 ◆ Specify a high-water mark for both the default data quota and the quotas set for users and groups.
	
	 Disabling Data Quota Enforcement
	
	 ◆ Deselect this to disable all data quota enforcement.

◆ **Default User Data Quota Size**	◆ This applies to users who do not have another data quota (user or group) that applies to them. Default is 100 MB.
◆ **Default High-Water Mark**	◆ When a user exceeds the data quota high-water mark (the default is 90% of the applicable data quota), a warning message displays on the user's profile page informing the user that he or she is approaching the data quota. ESN displays how many kilobytes of disk space are still available.

Field, Option, or Button	Information and/or Action
◆ **Add a Group** button	**IMPORTANT:** Group quotas override default quota settings. If users belong to more than one group, they are assigned the highest quota to which they are entitled through group membership. 1. Click this to add a group of users. 2. In the **Group** field, start typing the name of the group for which you want to set a quota, then click the group name when it appears in the drop-down list. Repeat this process to add additional groups for which you want to assign the same data quota. 3. In the **Quota** field, specify the disk space limit for the group. 4. Click **OK**, then click **Apply** > **Close** to save the group data quota settings.
◆ **Add a User** button	**IMPORTANT:** User quotas override default quota settings and the settings on any groups to which users belong. 1. Click this to add an individual user quota. 2. In the **User** field, start typing the name of the user for which you want to set a quota, then click the user's name when it appears in the drop-down list. Repeat this process to add additional users for which you want to assign the same data quota. 3. In the **Quota** field, specify the disk space limit for the user. 4. Click **OK**, then click **Apply** > **Close** to save the user data quota settings.

Managing the File Upload Size Limit

The file upload size limit conserves disk space on your Micro Focus ESN site because it prevents users from uploading large files to the ESN site. The default size limit for uploading files into your ESN site is 2 GB.

Path: Port 8443 ESN Admin Console **Management > File Upload Limits**

Table 11-3   Using the ESN Upload Limits dialog

Field, Option, or Button	Information and/or Action
Default File Upload Size Limit	◆ Unlike data quotas, there is no option to enable or disable file upload size checks. ◆ The default file upload size limit is 2 GB, but you can modify this if needed. ◆ You can also add different upload limits for individual users and groups as explained below.

Field, Option, or Button	Information and/or Action
◆ **Add a Group** button	**IMPORTANT:** Group upload limits override the default limit. If users belong to more than one group, they are assigned the highest upload limit to which they are entitled through group membership. 1. Click this to add a group of users. 2. In the **Group** field, start typing the name of the group for which you want to set an upload limit, then click the group name when it appears in the drop-down list. Repeat this process to add additional groups for which you want to assign the same upload limit. 3. In the **File Size Limit** field, specify the size limit for the group. 4. Click **OK**, then click **Apply** > **Close** to save the group file size limit.
◆ **Add a User** button	**IMPORTANT:** User upload limits override default upload limits and the limits set for any groups to which users belong. 1. Click this to add an individual user upload limit. 2. In the **User** field, start typing the name of the user for which you want to set an upload limit, then click the user's name when it appears in the drop-down list. Repeat this process to add additional users for which you want to assign the same upload limit. 3. In the **File Size Limit** field, specify the file size limit for the user. 4. Click **OK**, then click **Apply** > **Close** to save the user file size limit.

12 Product Improvement

The first time you log in to ESN, after changing the admin user's password, a dialog displays that explains that the purpose of the ESN data collection system is to help improve the ESN product.

The data collection process runs for the first time when a ESN appliance has been running for 24 hours. Thereafter, it runs weekly.

For additional information, see "Helping Micro Focus Improve ESN" in the *ESN 1.0: Maintenance Best Practices Guide*.

IMPORTANT: Micro Focus collects nothing that identifies your organization, your data, or your users.

Path: Port 8443 ESN Admin Console**Management > Product Improvement**

Table 12-1 *Using the Product Improvement dialog*

Field, Option, or Button	Information and/or Action
◆ **Collect and send the product name and version, and the number of LDAP users.**	◆ This option causes the ESN system to send Micro Focus information about the product version and build, license type, and number of users.

◆ **Also collect and send information about the deployment size and configuration, the number of files and folders, and so on.**	◆ This option causes the ESN system to send additional information about the installation, most of which is self-explanatory.
	
	    ◆ The **user** information doesn't include the LDAP user count because that is already available under the Tier1.
	    ◆ The user count numbers do not include system user accounts, such as `admin`, `_filesyncagent`, and so on.
	    ◆ The group count numbers do not include system groups, such as `allusers`, `allextusers`, and so on.
	    ◆ The numbers in `fileCounts` and `folderCounts` in the `netFolder` section correspond to each other by position.
	    ◆ The mobile device type is derived from the value of the description field associated with the device information captured in the system. Any descriptions that don't match one of the pre-defined keywords are included as `other`.

◆ **View the information collected.**	◆ After the system has been running 24 hours, this link displays so that you can download and review the `.json` file created by the collection process. This is the file that is sent to Micro Focus via FTP.

13 Search and Lucene Indexing

Indexing is key to all access within ESN, including files and folders, searching on content, and even users and groups.

For more information, see "ESN Search Appliance—Accessibility, and Searchability" in *ESN 1.0: Understanding How ESN Works*

This section covers the following:

- "Managing ESNsearch Configuration Settings" on page 65
- "Managing the Lucene Index" on page 66
- "Managing Search Nodes" on page 68
- "Managing Memcached (Search Index Appliance Only)" on page 68

Managing ESNsearch Configuration Settings

For more information, see "ESN Search Appliance—Accessibility, and Searchability" in *ESN 1.0: Understanding How ESN Works*

Path: Port 9443 ESN Appliance ConsoleConfiguration Icon > Search Appliance

Table 13-1 *Using the Search Appliance dialog*

Field, Option, or Button	Information and/or Action
Configuration Type:	The options that follow depend on the configuration type selected, as shown below.

◆ **Local**	◆ This is the default configuration type for a small ESN deployment, wherein the Lucene search index, the PostgreSQL database, and the ESN software are running on the same virtual machine.
	
	  ◆ **Host Name:** localhost indicates that the indexing process is running on the same appliance and the ESN process.
	  ◆ **RMI Port:** 1199 is the port used and cannot be changed.

◆ **Server**	◆ This option is for when only one Lucene search index is running as a stand-alone appliance.
	
	This is not a best practice configuration.
	
	  ◆ **Host Name:** The DNS host name of the stand-along search appliance..
	  This is set at install time.
	  ◆ **RMI Port:** 1199 is the default and Micro Focus does not recommend changing this.
	  ◆ **Lucene User Name:** The default name is `lucene service` but you can type a different name as long as you use the same name throughout your deployment.
	  ◆ **Lucene User Password:** The password for the Lucene user.

Field, Option, or Button	Information and/or Action

◆ **High Availability**	◆ Select this when two Lucene search indexes are running as stand-alone appliances.
	
	This is the best practice configuration.
	
	    ◆ **Lucene User Name:** The default name is `lucene service` but you can type a different name in the **User Name** field as long as you use the same name throughout your deployment.
	
	    ◆ **Lucene User Password:** The password for the Lucene user.
	
	NOTE: The following options apply to only High Availability configurations.

◆ **Add** button	◆ Click this to open the New Search Node dialog.
◆ **Remove** button	◆ Select a listed ESNsearch appliance by clicking in the white space of its row. Then click **Remove** to remove the appliance.
New Search Node	
◆ **Name**	◆ Specify a name for the Lucene search index appliance you are adding. You must specify the same name on each ESN appliance in the cluster. For example, if from one ESN appliance you secify `ESNsearch_index1` for this appliance, then you must secify `ESNsearch1_index1`) on each of the ESN appliances in the cluster.
◆ **Description**	◆ Specify a short description for the Lucene appliance.
◆ **Host Name**	◆ Specify the DNS host name or IP address of the ESNsearch appliance you are adding.
◆ **RMI Port**	◆ 1199 (informational only). (See Remote Method Invocation (http://java.sun.com/javase/technologies/core/basic/rmi/index.jsp).)
ESNsearch List	
◆ **Name**	◆ You can click this to open the New Search Node dialog.
◆ **Host Name**	◆ 1199 (informational only).
◆ **RMI Port**	◆ 1199 (informational only).
OK button	◆ To save your changes, click this, then click **Reconfigure ESN Server**. This stops and restarts your ESN server. Because this results in server downtime, you should restart the server at off-peak hours.
Cancel button	◆ Click this to cancel the changes you have made.

Managing the Lucene Index

The Lucene index provides access to all data in your Micro Focus ESN site, including objects, such as users, groups, files and folders, and file contents where content indexing is enabled.

For more information, see "ESN Search Appliance—Accessibility, and Searchability" in *ESN 1.0: Understanding How ESN Works*

Path: Port 8443 ESN Admin Console**Search Index > Index**

Table 13-2 *Using the Search Index page*

Field, Option, or Button	Information and/or Action
Manage Search Index tab	Use the options under this tab if users report that they can't find information or people that they know should be available in ESN. Chances are good that the index has become damaged or out-of-date for some reason.
	This is not a good option to correct slow performance. Re-indexing takes much longer and requires more resources than optimization (available in the Optimize Search Index tab).
	For more information, see "Rebuilding the Lucene Index" in the *ESN 1.0: Maintenance Best Practices Guide*.
◆ **Re-Index Everything**	◆ Use this option to rebuild all of the indexes for your entire site.
	◆ Keep in mind that no one will be able to access any of the files, folders, users, groups, etc. until a corresponding synchronization process has taken place and the metadata index for the items is re-created.
	◆ Depending on the size of your ESN site, this can be a very time-consuming process.
◆ **Select the Places to Be Re-Indexed:**	◆ If you know that there are problems with specific portion sof the site, you can choose to reindex only those portions.
◆ **Select the Nodes to Apply Re-Indexing to:**	◆ You can choose which of the appliances to apply the reindexing to.
	◆ Micro Focus recommends setting one of the nodes to write-only and reindexing only the other node. (See "Managing Search Nodes" on page 68.)
Optimize Search Index tab	Use the options under this tab if you notice that search performance in Micro Focus ESN is becoming slower over time.
	As a rule of thumb, you should run the optimization once a week during off hours or on weekends when the ESN system is not being heavily used.
	IMPORTANT: For optimization to run, there must be at least 51% free disk space on the Lucene search index appliance.
	Optimizing the Lucene index does not repair a damaged or out-of-date index. You must use the Manage Search Index tab in those cases.

◆ **Optimizing the Search Index**
  ◆ **Run Immediately**
  ◆ **Run at Scheduled Time**
	◆ You can either choose to run the optimization immediately, or schedule it during off hours or on weekends as the options indicate.

◆ **Select the Nodes to Apply Optimization to:**	◆ You can choose which of the appliances to apply the optimization to.

Managing Search Nodes

This dialog lets you control access to the ESNsearch appliances (search nodes) and is integral to certain index maintenance operations.

For example, you can take one Lucene node out of service for maintenance while other Lucene nodes continue to operate. Then you can synchronize the out-of-date Lucene node with the current indexing data.

For more information, see "Search Index Maintenance" in *ESN 1.0: Maintenance Best Practices Guide*

Path: Port 8443 ESN Admin Console**Search Index > Nodes**

Table 13-3 *Using the Search Nodes dialog*

Field, Option, or Button	Information and/or Action

◆ Node information
  ◆ *IP_address*
  ◆ **Host:**
  ◆ **RMI Port:**
	◆ This is informational only.

◆ **User Mode Access:**	◆ **Read and Write:** This is the normal operating mode and allows the ESN system to both retrieve information from the index and modify the index. ◆ **Write Only:** Select this if you are performing a re-index on the search index node. ◆ **No Access:** Selecting this option ensures that no data is written to the index while maintenance is being performed, such as upgrading the appliances or adding more disk space or memory
◆ **Enable Deferred Update Log**	◆ Do not deselect this unless instructed to do so by a support technician as part of resolving an incident report.

Managing Memcached (Search Index Appliance Only)

Path: Port 9443 Appliance Console**Memcached icon**

Table 13-4 <>

Field, Option, or Button	Information and/or Action
◆ **Listen Interface:**	◆ The URL that Memcached listens on.
◆ **Number of Threads:**	◆ The number of threads to use when processing incoming requests.
◆ **Max Memory:**	◆ Max memory that can be used by Memcached.
◆ **Max Simultaneous Connections:**	◆ Specify the number of network connections that can be handled by memcached simultaneously.

14 Security

Enterprise data is a critical resource that must be protected from unauthorized access, eavesdropping, corruption, unintended modification, or Trojan horses.

Generating, storing, and protecting enterprise data requires significant investments in time, money, and other resources.

ESN is designed to enhance an organization's ability to use and leverage its data. It has been carefully engineered to guard against exposing data to additional vulnerabilities.

- ◆ "Certificates" on page 69
- ◆ "Firewall Configuration" on page 69
- ◆ "Password Security (Local and External Users)" on page 70
- ◆ "User Visibility" on page 70
- ◆ "Viewing, Wiping, and Disconnecting Registered Clients" on page 71

Certificates

For certificate-maintenance procedures associated with this dialog, see Certificate Maintenance in the ESN 1.0: Maintenance Best Practices Guide

Path: Port 9443 Appliance Console**Digital Certificates icon**

Table 14-1   *Using the Digital Certificates Page*

Field, Option, or Button	Information and/or Action
Certificates in the Selected Key Store	
◆ **Key Store** drop-down	◆ Use this drop-down list to filter whether JVM or Web Application Certificates are listed.
◆ **File** drop-down	◆ This drop-down list lets you create a new key pair, import a trusted certificate or key pair, export a certificate you have selected in the list, or generate a CSR for a web application you have selected.
◆ **Edit** drop-down	◆ This exposes the option to delete a certificate you have selected.
◆ **View Info**	◆ This lets you view the information for a selected certificate
◆ **Reload**	◆ This lets you reload a selected certificate.

Firewall Configuration

Path: Port 9443 Appliance Console**Firewall icon**

Table 14-2 *Using the Firewall Details page*

Field, Option, or Button	Information and/or Action
Firewall Details	This page is only informational, not editable.
	It lists the port numbers that ESN expects to use on your network and the current status of each port.

Password Security (Local and External Users)

You can require that user passwords to the ESN site meet certain criteria by enabling password complexity checking. Only locally created users and external users are affected by this setting; users whose accounts are synchronized to ESN via LDAP are not affected.

Users' existing passwords are not forced to comply with the password policy; only when a user changes his or her password is the password policy put into effect.

Path Port 8443 ESN Admin Console**System > Password Policy**

Table 14-3 *Using the Configure Password Policy dialog*

Field, Option, or Button	Information and/or Action
Password complexity changing requires that passwords:	

◆ **Enable Password Complexity Checking for Local and External Users**	◆ When this is enabled, ESN requires that passwords:
	
	  ◆ Are at least 8 characters in length
	
	  ◆ Do not contain the user's first name, last name, or user ID (these restrictions are not case-sensitive)
	
	  ◆ Contain at least 3 of the following:
	
	    ◆ A lower-case character
	
	    ◆ An upper-case character
	
	    ◆ A number
	
	    ◆ One of the following symbols: ~ @ # $ % ^ & * ( ) – + { } [ ] | \ ? / , . < >

User Visibility

By default, each ESN user can see all other ESN users on the ESN site.

In a large organization it can be daunting for users to sort through a long list of people they don't work with to find those in their groups or on their teams.

ESN lets you restrict the users that appear in sharing dialogs and so on, to only those within groups to which a user belongs.

For a detailed explanation of ESN's User Visibility feature, see "Key Points About User Visibility in ESN" in *ESN 1.0: Understanding How ESN Works*.

Path: Port 8443 ESN Admin Console: **Management** > **Limit User Visibility**

Table 14-4 *Using the Limit User Visibility dialog*

Field, Option, or Button	Information and/or Action
◆ **Add Limitation**	◆ Click this, begin typing, select a listed user or group to limit them to seeing only other members of the groups they belong to.
◆ **Add Override**	◆ Click this, begin typing, select a listed user or group to enable them to see everyone.
◆ **Remove Visibility Settings**	◆ Select a user or group and click this to remove them from the list.
◆ **Filter List**	◆ Type a string within the user or group names to filter the displayed list to only those containing the string.
◆ **Gear icon**	◆ Select this to change the column sizes.
◆ **Limited Visibility On**	◆ Select the box next to the option to activate the visibility limitations for all listed users and groups. Or ◆ Select the users and groups you want to be affected by their limitations.

Viewing, Wiping, and Disconnecting Registered Clients

ESN lets you manage registered client devices from the ESN Administration Console.

You can remove devices from the registration list and schedule the removal (wiping) of all ESN data from the device the next time the user logs in.

For more detail, refer to the descriptions of dialog buttons, fields, and so on in Table 14-5.

Path: Port 8443 ESN Admin Console**Management > Registered Clients**

Table 14-5 *Using the Registered Clients dialog*

Field, Option, or Button	Information and/or Action
Registered Clients - System Wide	
◆ **Delete** button	◆ Click this to remove a device from the list. This doesn't affect the device, only its registration status with ESN. The device is re-registered if the user logs in again.
◆ **Wipe** drop-down	◆ **Schedule Devices to be Wiped:** If you select this, then the next time the user logs in to the device, the user password and all online and available-offline files are removed from the device. The ESN application then exits, but it is not uninstalled or removed from the device. ◆ **Clear Scheduled Wipe from Devices:** This removes the scheduled wipe and no information is removed the next time the user logs in to the device.

Field, Option, or Button	Information and/or Action
◆ **Device Name**	◆ The name given to the device by the device owner.
◆ **OS Version**	◆ The operating system on the device.
◆ **Client**	◆ The version of the ESN application that is installed on the registered device.
◆ **User**	◆ The name of the ESN user who logged in from the listed device.
◆ **Last Login**	◆ The date and time when the device was last used to log in to the ESN system.
◆ **Wipe Scheduled**	◆ This indicates whether a wipe has been scheduled to occur so that all ESN data is removed from the device the next time the user logs in from it.
◆ **Last Wipe**	◆ The last time ESN data was wiped from the device.
◆ **Filter List**	◆ Filter the displayed list by typing a string found in any of the rows. For example, you could type "7" to see a list of Windows 7 registered clients.
◆ Gear icon	◆ Click this to access the Edit Column Sizes dialog.

15 Sharing

The following sections cover the main administrative controls for sharing in ESN.

Managing Shared Items

Use this dialog to manage the share settings for all shared files and folders.

Path: Port 8443 ESN Admin Console**Management > Shares**

Table 15-1   *Using the Shares dialog*

Field, Option, or Button	Information and/or Action
Manage Shares	
Find share items by: drop-down list	◆ Use this to filter the list of shares by one of the options below.
◆ **User**	◆ Begin typing the name of a user in the **User** field, then select the user name when it appears in the drop-down list. All active shares from that user are displayed in the table.
◆ **File**	◆ Begin typing the name of a file in the **File** field, then select the file name when it appears in the drop-down list. All active shares associated with that file are displayed in the table.
◆ **Folder**	◆ Begin typing the name of a folder in the **Folder** field, then select the folder name when it appears in the drop-down list.
	◆ Or click the **Browse** icon next to the **Folder** field and browse to the folder. All active shares associated with that folder are displayed in the table.
◆ **Find all shares**	◆ Select this to display all active shares in the ESN system.
Shared With sub-section	◆ This section lists all of the shared items and who has access to them.
	◆ You can also use the checkbox next to this label to select all of the listed shares.
	After the shares are selected, you can modify the shared-access rights.
◆ **Delete** button	◆ Use this to remove any of the listed shares from the list. Only the share is removed, shared items themselves are not affected.
◆ **Access Rights**	◆ After selecting a shared item, you can decrease the granted access rights or increase them within the limits available to the user who shared the item.
◆ **Allow re-share with**	◆ You can adjust the re-share privileges within the limits available to the user who shared the item.

Field, Option, or Button	Information and/or Action
◆ **Expires**	◆ You can adjust the expiration so that the share never expires, expires on a certain date, or expires after a specified number of days.
◆ **Note:**	◆ You can include a note about the changes you have made. This will then be distributed according to the option that you select for the **Notify** option.
◆ **Notify:**	◆ You can choose among four notification options: ◆ **All recipients:** An email that includes your note is sent to all of those with the share. ◆ **Only newly added recipients:** An email that includes your note is sent to newly added recipients. ◆ **New and modified recipients:** An email that includes your note is sent to all newly added recipients and those whose privilges have changed . ◆ **None:** No email is sent.
OK button	◆ Click this to save your changes and send notifications as specified.
Cancel button	◆ Click this to cancel the changes you have made.

Managing Sharing, License Terms, and Comments

For users to be able to share files and folders in ESN, they must be enabled directly or as a group member through this dialog.

My Files sharing is then automatic for those listed, unless explicitly restricted.

Path: Port 8443 ESN Admin Console**System > Share and Comment Settings**
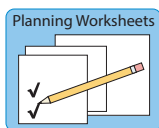
Best Practice: Plan sharing in advance and use the following worksheets when working in this dialog:

◆ Worksheet 14 - System-Level Sharing Settings

Table 15-2   Using the Share and Comment Settings dialog

Field, Option, or Button	Information and/or Action
Share and Comment Settings dialog	
Rights tab	For a graphical explanation of the settings in this tab, see "The Rights Tab Controls All ESN Sharing" on page 76.
◆ **Allow all users to share with groups that have been imported from LDAP**	◆ If you select this option, groups that were imported from the LDAP directory are displayed in the **Share with** field when users are sharing an item (as described in "Sharing Files and Folders" in the *ESN 1.0: User Access Guide*). All users in the LDAP group then have access to the item that was shared.

Field, Option, or Button	Information and/or Action
◆ **User or Group:**	**IMPORTANT:** For users or groups to share items in ESN, they must be listed here. ◆ Begin typing a user or group name and then select it in the list. The Grant Share Rights dialog displays.

◆ User/Group List
   ◆ **Name**
   ◆ **Rights**
   ◆ **Type**
	◆ This lists the users and groups that are granted rights to share files and folders in ESN.
	
	◆ Users that are listed individually and also as members of groups have all of the rights that are granted in their applicable listings.

Grant Share Rights dialog	
◆ **Re-share items**	◆ When users share a file or folder, they can give the users they are sharing with the ability to re-share the file or folder. **IMPORTANT:** Excercise caution here because even a user's access rights to an item are removed, that does not remove the access rights of the user with whom the item was re-shared.
◆ **Share with internal users**	◆ Lets users share items with internal users.
◆ **Share with "All Internal Users" group**	◆ Lets users perform a mass share to all internal users by sharing with the `All Internal Users` group.
◆ **Share with External Users**	◆ Lets users share items with users external to the organization through the external users' email addresses. ◆ Email notifications include a link to the shared item. Users can then log in to the ESN site and self provision. For more information, see "Sharing with People Outside Your Organization" in the *ESN 1.0: User Access Guide*.
◆ **Share with the Public**	◆ Lets users make items publicly available. Anyone with the URL to the ESN site can access the Public folder and see the item along with everything else in the folder. Public access requires that you enable Guest access to the ESN site. For information about how to enable Guest access to the ESN site, see "Web Browser Access—Default Settings" on page 23
◆ **Share using File Link**	◆ Lets users share a link to a file in ESN. Any user with the link can then access the file. The file is not displayed in the Public area, so users must have direct access to the link in order to access the file. For more information about File Links, see "Distributing a Link to a File" in the *ESN 1.0: User Access Guide*.
Whitelist / Blacklist tab	
Mode	
◆ **No restrictions**	◆ Lists are ignored and users can share with any email address.
◆ **Whitelist**	◆ Allows sharing only with email addresses and domains that have been specified in the **Email addresses** and **Domains** fields.

Field, Option, or Button	Information and/or Action
◆ **Blacklist**	◆ Disallows sharing with any email addresses and domains that have been specified in the **Email addresses** and **Domains** fields.
◆ **Email addresses** list	◆ Use the **Add** and **Delete** buttons to add and remove email addresses from the list.
◆ **Domains** list	◆ Use the **Add** and **Delete** buttons to add and remove domains (such as yahoo.com) from the list.
◆ **Delete shares that don't meet the criteria**	◆ Select this option to delete all existing shares in the ESN system that do not match the criteria you set. For example, if you selected **Blacklist** and then specified **yahoo.com** in the **Domains** field, selecting this option would delete all ESN shares made to Yahoo email addresses.
External Users Licensing Terms tab	
◆ **Display Terms and Conditions**	◆ This tab lets you require that any external users who access the ESN site after receiving an email invitation accept the terms and conditions that you specify in the field provided before being granted access. **IMPORTANT:** This does not apply to Guest (Public) access.
Comment Settings tab	
◆ **Allow Commenting on Files.**	◆ Disabling this option prevents all users from logging comments in ESN. ◆ You can also disable commenting for only Guest (Public) users. See "Guest access is read only" on page 23.
OK button	◆ Click this to save your changes.
Cancel button	◆ Click this to cancel the changes you have made.

The Rights Tab Controls All ESN Sharing

To use ESN sharing, users must listed here, either individually or as a member of a group.

2. Begin typing a user or group name.

1. Select this option to let Filr users share with all LDAP-imported groups.

3. Select a name to add it to the list.

Share Settings

| Rights | Whitelist / Blacklist | External Users Licensing Terms |

☐ Allow all users to share with groups that have been imported from LDAP

Select a user or group to add to the list and then grant share rights.

User or Group: bl

| Name | Rights | Type |
| blackknight | Internal / External / Share File Link ▾ | User ⊗ |

OK   Cancel

bl
👤 Black Knight (blackknight)
👤 Black Knight (black (ad))
👤 Blue Moon (bluemoon)
👤 Blue Moon (blue (ad))

◉ 1-4 of 4 ◉

4. Specify the maximum Filr sharing rights for the user or group.

You cannot grant rights elsewhere that aren't granted here.

For example, Black Knight will not be allowed to reshare items that have been shared with him unless that right is added here.

5. Repeat from Step 2 until all users who need to share have been granted sharing rights.

Grant Share Rights

Recipients will be granted share rights to:

☐ Re-share items
☑ Share with Internal users
   ☐ Share with "All Internal Users" group
☑ Share with External users
☐ Share with the Public
☑ Share using File Link

OK   Cancel

16 SQL Database Connection

ESN uses the SQL database for storing file and folder, and user and group metadata. You can change any of the fields in this dialog to match corresponding changes to the database server.

Path: Port 9443 Appliance Console**Configuration icon > Database**
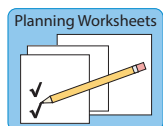
Best Practice: Plan your SQL database configuration in advance and use the following worksheets when working in this dialog:

- Worksheet 23 - SQL Database

Table 16-1 *Using the Database Connection dialog*

Field, Option, or Button	Information and/or Action
Database Connection dialog	Worksheet 23 - SQL Database Connection

◆ **Database Type:**	◆ Select the appropriate option for the database server.
	   ◆ **PostgreSQL:** Select **PostgreSQL**
	   ◆ **Microsoft SQL Server:** Select **MS SQL Server**

◆ **Host Name or IP Address:**	◆ The DNS host name or IP address of your SQL server.
◆ **Port:**	◆ The port used for communications with ESN. The standard port for the database type is automatically selected.
◆ **User Name:**	◆ The user id that ESN uses to log in to the database server.
◆ **User Password:**	◆ The password for the User Name.
◆ **Encrypt Database Communication:**	◆ Select this option to encrypt data communication from the ESN server to the database server. For more information, see "Database Communication Encryption" in the *ESN 1.0: Maintenance Best Practices Guide*.
OK button	◆ Click this to save your changes. Then click **Reconfigure ESN Server** so that the changes are used by ESN.
Cancel button	◆ Click this to cancel the changes you have made.

17 Storage Management

◆ "Expanding Storage" on page 81

Expanding Storage

Path: Port 9443 Appliance Console**Storage icon**

Table 17-1   *Using the Storage Expansion dialog*

Field, Option, or Button	Information and/or Action
Prerequisite	◆ Storage expansion requires unallocated free disk space associated with the `/vastorage` and/or `/var` partitions.
	◆ Use the tools and processes provided by your hypervisor vendor to expand the virtual disks that contain the partitions you want to expand.
	◆ Restart the appliance so that the operating system can detect the disks that have been expanded.
Appliance Disks Containing Unallocated Free Space: If no disks are listed, nothing is available to be expanded.	
Expand partitions	◆ After selecting the devices you want to expand, click this option.
	Appliance services are stopped, the selected partitions are expanded to the size of their respective disks, and appliance services are restarted.
	◆ Restart the appliance again so that the management software detects that the unallocated disk space has been used.

18 Support Files and Online Updates

Managing Field Test Patches

You can manage field test patches for the ESN appliance directly from the appliance. You can install new patches, view currently installed patches, and uninstall patches.

Path: Port 9443 Appliance Console**Field Patch icon**

Table 18-1 *Using the Field Patch dialog*

Field, Option, or Button	Information and/or Action
Field Test Patch	
Install a Downloaded Patch sub-section	
• **Path to Field Patch:**	• Use the **Browse** button to navigate to a downloaded patch, then click **Install** to apply the patch.
Manage Installed Patches sub-section	• This lists all of the patches that are currently installed, when they were installed, and information about the patch as supplied by Micro Focus.
• **Uninstall Latest Patch** button	• Patches must be uninstalled in reverse order and only the latest patch can be uninstalled.
	• Select the latest installed patch, then click this button and confirm that you want the patch uninstalled.
	You can then install the next patch until you have everything uninstalled as required.
• **Download Log File** button	• Click this to download the log file that tracks patch installations.

Managing Online Updates

Path: Port 9443 Appliance Console**Online Update icon**

Table 18-2 *Using the Online Update dialog*

Field, Option, or Button	Information and/or Action
Online Update (Automatic Update Schedule: *X***)**	◆ This is the dialog title and it also shows which Schedule option is selected (represented by *X*).
Register Online Update Service dialog	◆ This dialog appears whenever the appliance is not registered with an update service. For example, the first time Online Update icon is clicked or when a service has been de-registered. ◆ You must register the appliance for it to receive online updates.
◆ **Service Type:**	◆ Select the service type that the appliance will use to obtain online updates: a local Subscription Management Tool (SMT) or the Micro Focus Customer Center
◆ **Local SMT**	This is a server from where you can download the software updates and automatically install them to update the product. ◆ **Hostname:** The hostname of the server from where you want the appliance to download software updates. ◆ **SSL cert URL (optional):** The path to the SSL certificate for encrypting communications with the server. ◆ **Namespace path (optional):** To enable the client to use the staging group, specify a value. Do not specify any value if you want to use the default production repositories.

◆ **Micro Focus Customer Center**	◆ **Email:** Your email address for registering the appliance to receive updates.
	
	◆ **Activation Key:** This displays in your NCC Portal in the same dialog as your product license.
	
	◆ **Allow Data send:** Select from the following options if you want to share information with the Micro Focus Customer Center:
	
	    ◆ **Hardware Profile:** Shares the hardware information.
	
	    ◆ **Optional Information:** Shares information such as host type, productversion, release, architecture, timezone, and processor.

Update service: *X*	◆ After you register the appliance for an update service, the service name appears in this field (represented by *X*).
◆ Patches drop-down	◆ **Needed Patches:** Selecting this option lists that patches that will be installed during the next manual or automatic update. ◆ **Installed Patches:** Selecting this option lists all patches that have been previously installed.
◆ **Schedule** drop-down	◆ Click this to set a schedule for when the appliance will download updates. ◆ If you select **Manual**, the appliance immediately downloads all available patches. ◆ If you select **Daily**, **Weekly**, or **Monthly**, you must then choose to apply either **All Needed Patches** or **Security Patches Only**. ◆ Optionally, you can specify whether to **Automatically agree with all license agreements** and **Automatically install all interactive patches**.

Field, Option, or Button	Information and/or Action
Update Now tab	◆ This is selectable only when the Patches drop-down is set to **Needed Patches**. ◆ After clicking the option, you must choose to apply either **All Needed Patches** or **Security Patches Only**. ◆ Optionally, you can specify whether to **Automatically agree with all license agreements** and **Automatically install all interactive patches**.
View Info tab	◆ Clicking this displays information such as a brief summary of the patch and the bug fixes in the patch.
Register tab	◆ Clicking this displays the appliance's registration status, and an option to **Deregister** the appliance. ◆ If you deregister the appliance, the Register Online Update Service dialog reappears.
Refresh tab	◆ Clicking this refreshes the status of updates on the Appliance.

Submitting Configuration Files to Micro Focus Support

Sometimes Micro Focus Support needs to review your appliance's system configuration when processing a service request. This dialog facilitates the process and saves you time.

Path: Port 9443 Appliance Console**Support icon**

Table 18-3   Using the Support dialog

Field, Option, or Button	Information and/or Action
Support	
Automatically send the configuration to Micro Focus using FTP.	◆ With this option selected, you can FTP your configuration to Micro Focus Support and include the **Service Request Number** if desired. ◆ The configuration is sent when you click **OK** and confirm your selection.
Download and save the configuration file locally, then sent it to Micro Focus manually.	◆ With this option selected, the configuration is downloaded when you click **OK** and confirm your selection. ◆ You must then send the file to Micro Focus through email or some other arrangement.
OK or **Cancel**	◆ Click **OK** to send or download the file, or click **Cancel** to exit.

19 Changing System Services Configurations

Managing System Services

Path: Port 9443 Appliance Console**System Services icon**

Table 19-1 *Using the System Services dialog*

Field, Option, or Button	Information and/or Action
Available System Services: This varies by appliance type as listed below this table.	
◆ **Action** drop-down	◆ Use this to **start**, **stop**, or **restart** the selected service. Before doing any of these, make sure you understand how your action will affect the appliance.
◆ **Options** drop-down	◆ Use this to set the selected service to start automatically or require a manual start.
◆ **Refresh List**	◆ Click this if the information displayed is outdated.

ESN Appliance

- **SSH:** This is the SSH service that is running on the appliance.
- **Micro Focus ESN:** This is the ESN service that is running on the appliance. Click **Download** to access the `appserver.log` and `catalina.out` files.
- **Jetty:** This is the Jetty service that is running on the appliance. Click **Download** to access the `jetty.stderrout.out` file.
- **PostgreSQL:** This is the PostgreSQL service that is running on the appliance. Click **Download** to access the `PostgreSQLd.log` file.

  The PostgreSQL service runs on the ESN appliance in a small deployment, and on the PostgreSQL appliance in a large deployment.

Lucene Search Index Appliance

- **SSH:** This is the SSH service that is running on the appliance.
- **Jetty:** This is the Jetty service that is running on the appliance. Click **Download** to access the `jetty.stderrout.out` file.
- **Search:** Click **Download** to access the `indexserver.log` file
- **Memcached:** Click **Download** to access the `jetty.stderrout.out` file.

PostgreSQL Database Appliance

- ◆ **SSH:** This is the SSH service that is running on the appliance.
- ◆ **Jetty:** This is the Jetty service that is running on the appliance. Click **Download** to access the `jetty.stderrout.out` file.
- ◆ **PostgreSQL:** This is the PostgreSQL service that is running on the appliance. Click **Download** to access the `PostgreSQLd.log` file.

Shutting Down and Restarting the Micro Focus Appliance

Path: Port 9443 Appliance Console**Reboot** or **Shutdown**

- ◆ **Reboot:** Use this if you need to restart the Micro Focus appliance after performing maintenance.
- ◆ **Shutdown:** To ensure that appliance processes are properly terminated, you should always use this when you need to shutdown a Micro Focus appliance.

  Using the hypervisor's management features to power down or restart an appliance can result in system corruption.

20 Time and Locale

Changing the Appliance's NTP Configuration

This dialog lets you adjust the NTP configuration settings that were established when the appliance was deployed.

Path: Port 9443 Appliance Console**Time icon**

Table 20-1 Using the Time dialog

Field, Option, or Button	Information and/or Action
◆ **NTP Servers:**	◆ Type a new default NTP server.
◆ **Region:**	◆ Click the drop-down list and select a region for the appliance.
◆ **Time Zone:**	◆ Click the drop-down list and select a time zone for the appliance.
◆ **Hardware clock set to UTC**	◆ Use this option to change the hardware clock setting.

Setting a Default Time and Locale for Non-LDAP and External Users

NOTE: You specify the default locale and time zone for LDAP users when you configure LDAP synchronization.

On the other hand, when you create non-LDAP internal users and when external users self-provision, ESN assigns `English (US)` as the default locale and `Greenwich Mean Time (GMT)` as the default time zone.

This dialog lets you change the non-LDAP internal user and external user defaults.

Path: Port 8443 ESN Admin Console > **Management > Default User Settings**

Table 20-2 Using the Default User Settings dialog

Field, Option, or Button	Information and/or Action
Section: Settings for new internal (non-LDAP) users:	
◆ **Time Zone:**	◆ Use the drop-down list to select a default time zone for ESN to assign when you create Internal, non-LDAP users.

Field, Option, or Button	Information and/or Action
◆ **Locale:**	◆ Use the drop-down list to select a default locale for ESN to assign when you create Internal, non-LDAP users.
Section: Settings for new external users:	
◆ **Time Zone:**	◆ Use the drop-down list to select a default time zone for ESN to assign when external users self-provision to ESN.
◆ **Locale:**	◆ Use the drop-down list to select a default locale for ESN to assign when external users self-provision to ESN.
OK or **Cancel**	◆ Click **OK** to apply the settings you have specified and exit this dialog, or **Cancel** to discard your changes and exit.

21 UI Controls and Customizations

Email Notification Template Customization

You can customize the email notifications that ESN generates as part of your branding efforts, to provide localized messages, to comply with organizational policies, and so on.

For more information about the templates, see "Notification (Email) Customization" in the *ESN 1.0: Maintenance Best Practices Guide* and "Email Template Customization—A Video Walkthrough" in *ESN 1.0: Maintenance Best Practices Guide*.

Path: Port 8443 ESN Admin Console > **System > Email Templates**

Table 21-1   Using the Manage Email Templates dialog

Field, Option, or Button	Information and/or Action
◆ **Delete** button	◆ This button is activated when you select a template in the list that has been customized. ◆ Use it to delete a customized template that you have uploaded to ESN by using the **Add Files** button. Removing a customized template causes ESN to revert to using the default template that ships with ESN.
◆ **Add Files** button	◆ Use this to upload a customized template file to the ESN system.
◆ **Name**	◆ The names of the email templates that ESN uses.
◆ **Type**	◆ This indicates whether ESN is using a customized or default template.
◆ **Gear** icon	◆ This lets you adjust column sizes on this page.

HTML Rendering of Non-HTML Files

Path: Port 9443 Appliance Console **Configuration > HTML Viewing**

Table 21-2 *Using the HTML Viewing dialog*

Field, Option, or Button	Information and/or Action
◆ **Default HTML Extensions:**	◆ This lists the file extensions that ESN automatically renders as HTML.
◆ **Additional HTML Extensions:**	◆ You can specify additional extensions, separated by commas, that you want ESN to attempt to render as HTML. ◆ The extensions you enter remain in the field after you apply them, so that you can add to or remove items as you test whether they are useful additions to the defaults, or not.
OK and Cancel buttons	◆ After clicking **OK**, you must then click **Reconfigure ESN Server** for the changes that you've made to be applied. Or ◆ Click **Cancel** to discard your changes to the list of extensions in the **Additional HTML Extensions** field.

Branding the Desktop Apps

As the built-in Port 8443 administrator, you can brand your ESN mobile apps to match your organization's brand.

IMPORTANT: Direct Port 8443 administrators do not have rights to administer branding.

To customize desktop application branding, you must first create a branding file and then upload the file to the ESN server.

Path: Port 8443 ESN Admin Console > **System > Desktop Site Branding**

Table 21-3 *Using the Desktop App Branding dialog*

Field, Option, or Button	Information and/or Action
◆ **Mac Branding File**	**IMPORTANT:** You must first create a .zip branding file for your Mac desktops as outlined in "Desktop Branding Files" in the *ESN 1.0: Maintenance Best Practices Guide*. ◆ **Choose File** button Click this to choose the .zip file that you created for your Mac workstations as mentioned above. ◆ **Apply** button Click this to apply the branding .zip file you have created. If you choose to apply a different branding file without remove the existing branding, then a dialog prompts you that the existing branding file will be overwritten. Click **Yes** to overwrite the branding file or click **No** to retain the existing branding. ◆ **Remove Current Branding** button To remove an existing branding for the Mac desktop application, click the **Remove Current Branding** option.

Field, Option, or Button	Information and/or Action
◆ **Windows Branding File**	**IMPORTANT:** You must first create a .zip branding file for your Windows desktops as outlined in "Desktop Branding Files" in the *ESN 1.0: Maintenance Best Practices Guide*.
	◆ **Choose File** button
	Click this to choose the .zip file that you created for your Windows workstations as mentioned above.
	◆ **Apply** button
	Click this to apply the branding .zip file you have created.
	If you choose to apply a different branding file without remove the existing branding, then a dialog prompts you that the existing branding file will be overwritten. Click **Yes** to overwrite the branding file or click **No** to retain the existing branding.
	◆ **Remove Current Branding** button
	To remove an existing branding for the Windows desktop application, click the **Remove Current Branding** option.

Branding the Mobile Apps

As the built-in Port 8443 administrator, you can brand your ESN mobile apps to match your organization's brand.

IMPORTANT: Direct Port 8443 administrators do not have rights to administer branding.

Path: Port 8443 ESN Admin Console > **System > Mobile Site Branding**

Table 21-4   Using the Mobile App Branding dialog

Field, Option, or Button	Information and/or Action
◆ **iOS Branding File**	**IMPORTANT:** You must first create a .zip branding file for your iOS mobile devices as outlined in "iOS UI Branding" in the *ESN 1.0: Maintenance Best Practices Guide*.
	◆ **Choose File** button
	Click this to choose the .zip file that you created for your iOS mobile devices as mentioned above.
	◆ **Apply** button
	Click this to apply the branding .zip file you have created.
	If you choose to apply a different branding file without remove the existing branding, then a dialog prompts you that the existing branding file will be overwritten. Click **Yes** to overwrite the branding file or click **No** to retain the existing branding.
	◆ **Remove Current Branding** button
	To remove an existing branding for the iOS mobile devices, click the **Remove Current Branding** option.

Field, Option, or Button	Information and/or Action
◆ **Android Branding File**	**IMPORTANT:** You must first create a .zip branding file for your Android mobile devices desktops as outlined in "Android UI Branding" in the *ESN 1.0: Maintenance Best Practices Guide*.

◆ **Choose File** button

Click this to choose the .zip file that you created for your Android mobile devices as mentioned above.

◆ **Apply** button

Click this to apply the branding .zip file you have created.

If you choose to apply a different branding file without remove the existing branding, then a dialog prompts you that the existing branding file will be overwritten. Click **Yes** to overwrite the branding file or click **No** to retain the existing branding.

◆ **Remove Current Branding** button

To remove an existing branding for the Android mobile devices, click the **Remove Current Branding** option.

Branding the Web Client

As the built-in Port 8443 administrator, you can brand your ESN mobile apps to match your organization's brand.

IMPORTANT: Direct Port 8443 administrators do not have rights to administer branding.

When you add a site-wide brand to your ESN site, the brand is displayed on every ESN page. You can create your brand by adding an image, by creating the brand in HTML using CSS styles, or by using a combination of both.

Path: Port 8443 ESN Admin Console > **System > Custom Branding > Site Branding**

Table 21-5 *Using the Mobile App Branding dialog*

Field, Option, or Button	Information and/or Action
◆ **Use Branding Image:**	**IMPORTANT:** Images must be uploaded to ESN before they can be used for branding. You can upload them using this option or the **Background Image** option below. ◆ Select this option if you want to use the drop-down list to select an existing image for the branding foreground, such as a company or organizational name. By default, an image showing "Micro Focus ESN" displays here. If you replace this image, or select None, **Powered by Micro Focus ESN** displays below the user's name in the upper-right corner. ◆ To add image files to File, click the **Browse** icon ⬚. ◆ In the Add File Attachment dialog, use the Choose File button to browse to and select your branding images. If you want to upload multiple images, use the **Add file** button to add entries to the list of files to be uploaded.
◆ **Use Advanced Branding:**	◆ Select this option if you want to include advanced features, such as HTML and CSS styles in your branding.
◆ **Edit Advanced** button	◆ Click this to open the built-in editor and create your brand using uploaded images, HTML, and so on.
◆ **Background Image:**	◆ The background image displays behind your branding image or your advanced branding created above. ◆ **TIP:** Buttons in the header (such as My Files, and Shared with Me) display better when your background image is a medium to darker color. Lighter images make it more difficult to see the buttons. ◆ Images are available in the drop-down list after you upload them by clicking the **Browse** icon ⬚.
◆ **Stretch Image:**	◆ Use this option to stretch the background image to occupy the entire branding area.
◆ **Background Color:**	◆ Use this to add a background color that occupies the entire branding area. ◆ Rather than typing an RGB value or HEX number, use the color picker icon ⬚ to the right of this field to select the new color. ◆ If you added a background image and stretched the image, the background color is not displayed.
◆ **Text Color:**	◆ Use this to specify the text color of the workspace name in the upper-right corner of the branding area. ◆ Rather than typing an RGB value or HEX number, use the color picker icon ⬚ to the right of this field to select the new color.
Sign-in Dialog Image sub-section	
◆ **Current Image:**	◆ If you haven't already done so, browse to and select the image that you want to upload for the Login dialog. The suggested image size is width: 400px, height: 60 px.

Field, Option, or Button	Information and/or Action
◆ **Clear Branding** button	◆ Click this to clear all your branding customizations and restore the default Micro Focus ESN branding.
OK or Cancel	◆ Click **OK** to apply your changes, or **Cancel** to discard them. Canceling doesn't remove uploaded image files.

UI Language

For more information about UI language settings in ESN, see "Language Settings" in the ESN 1.0: Maintenance Best Practices Guide.

Path: Port 9443 Appliance Console**Configuration icon > Default Locale**

Table 21-6 *Using the Default Locale dialog*

Field, Option, or Button	Information and/or Action

◆ **Default Locale:**	◆ Use this option to reset the language that you selected during the ESN configuration process.
	
	The following points explain more about the **Default Locale** setting.
	
	  ◆ Micro Focus appliance installations run in English only.
	
	  ◆ When you install the ESN software, you can set the primary language, thereby establishing the UI language for text in locations where all ESN users see it, such as in the Workspace tree.
	
	    Your choices are:
	
	      ◆ Chinese-Simplified
	      ◆ Chinese Traditional
	      ◆ Czech
	      ◆ Danish
	      ◆ Dutch
	      ◆ English
	      ◆ French
	      ◆ German
	      ◆ Hungarian
	      ◆ Italian
	      ◆ Japanese
	      ◆ Polish
	      ◆ Portuguese
	      ◆ Russian
	      ◆ Spanish
	      ◆ Swedish
	
	  ◆ The language that you select or change here also establishes the default interface language and locale for new user profiles that are imported through LDAP.
	
	    The default language for non-LDAP and self-provisioned users is set in the Default User Settings dialog.

Name Completion Settings—Managing How Group Names Display in Drop-Down Lists

ESN includes a name completion (or Type-to-Find) feature that displays the names of users or groups as you begin typing a name or string.

For example, as you share an item and begin typing in the **Share with field**, names of users or groups that match what you have typed so far display so that you can select a listed item.

To help you distinguish between multiple groups with the same name, ESN includes secondary information.

This dialog lets you specify how group names are displayed in the drop-down list.

Path: Port 8443 ESN Admin Console**System > Name Completion Settings**

Table 21-7   *Using the Name Completion Settings dialog*

Field, Option, or Button	Information and/or Action

◆ **Primary display text:** drop-down list	◆ Click the drop-down list and select either
	
	  ◆ **Name:** The name of the group as it appears in ESN.
	
	  Or
	
	  ◆ **Title**: The title as it appears in the LDAP directory.

◆ **Secondary display text:** drop-down list	◆ Click the drop-down list and select either
	
	  ◆ **Description**: The description of the group as it appears in ESN.
	
	  Or
	
	  ◆ **Fully Qualified DN**. The Fully Qualified Domain Name as it appears in the LDAP directory.

22 Users and Groups

Managing Users

Path: Port 8443 ESN Admin Console **> Users**

Best Practice: Plan users in advance and use the following worksheets when working in this dialog:

◆ Worksheet 4 - Users and Groups

Table 22-1 *Using the Users dialog*

Field, Option, or Button	Information and/or Action
Users dialog (header row)	
◆ **New** button	◆ Click this to begin creating a new non-LDAP internal user.
◆ **Import Profiles...** button	◆ You can manage local users and groups by importing profile files that contain user or group information in XML format. This is a good way to simultaneously perform multiple actions on non-LDAP users and group, such as creating, modifying, or deleting users, and creating or modifying groups.
	◆ Click **Choose File**, then navigate to and select the file that contains user or group profile information in XML format.
	◆ Click **View a Sample File** and make sure that the format of your file matches the format that is shown in the provided sample file.
◆ **Delete** button	◆ The effects of this button on user accounts depends on whether the user is an LDAP, non-LDAP Internal, or External user. For more detail, see Deleting ESN Users in the ESN 1.0: Maintenance Best Practices Guide.

Field, Option, or Button	Information and/or Action
◆ **More** drop-down	With one or more users selected, you can choose from the following options. ◆ **Disable User Account:** Disabling ESN User Accounts in the ESN 1.0: Maintenance Best Practices Guide ◆ **Enable User Account:** This restores access through a user account that was previously disabled. ◆ **Disable Web Access:** "Web Browser Access—Individual Users and Groups" on page 23 ◆ **Enable Web Access:** "Web Browser Access—Individual Users and Groups" on page 23 ◆ **Use Default Web Access Setting:** "Web Browser Access—Individual Users and Groups" on page 23 ◆ **Desktop Application Settings...:** "Desktop Access—Individual Users and Groups" on page 17 ◆ **Mobile Application Settings...:** "Mobile Device Access—Individual Users and Groups" on page 20 ◆ **Add Administrator Rights:** Lets you assign selected users as Designated Administrators. ◆ **Remove Administrator Rights:** Lets you remove Direct-administration rights from selected users.
◆ **Filter List** field	◆ Begin typing a name and press enter to filter the list to only those users who match what you have entered.
◆ Filter Arrow drop-down	◆ This lets you filter the displayed list of users using the following criteria: ◆ Internal Users ◆ External Users ◆ Disabled Users ◆ Enabled Users ◆ Administrators ◆ Non-administrators By default, all of the above are selected for display.
◆ Gear icon	◆ Click this to adjust column sizes.
◆ Trash Can icon	◆ This displays a list of Personal Workspace trash items that can be recovered. ◆ **Restore** button: This lets you undelete selected items. ◆ **Delete** button: This lets you permanently erase the selected items. ◆ **Restore All** button: This restores everything in Personal Workspace trash. ◆ **Delete All** button: This permanently erases everything in Personal Workspace trash.

Users List (below header row)

◆ **Full Name** column	◆ Displays the user's first and last names combined

Field, Option, or Button	Information and/or Action
◆ Arrow drop-down column	◆ Provides access to the following settings for the user: 　◆ **User Properties** dialog: Opens the User Properties dialog. 　◆ **Web Access** settings: Depending on what has already been configured, you can enable web access for the user, disable web access for the user, or specify that the default web access settings be used for the user.
◆ **Type** column	◆ Icons indicate whether users are LDAP, non-LDAP internal, External self-provisioned, System-created, and so on.
◆ **Admin** column	◆ This indicates whether users are assigned administrative responsibilities.
◆ **Email** column	◆ This displays the email address to which ESN sends notifications
◆ Device Icon column	◆ Click this to view the Registered Clients list filtered to include only this user. This lets you manage all the user's devices from one place. For more detail, see "Viewing, Wiping, and Disconnecting Registered Clients" on page 71.
◆ **User Id** column	◆ The login name of each user
New User dialog	
◆ **User ID**	◆ You must assign a unique user ID for each non-LDAP internal user.
◆ **Password**	◆ You must assign (type and confirm) a password for the user to log in with.
◆ **First Name**	◆ You can include the user's first name
◆ **Last Name**	◆ You can also include the user's last name.
◆ **Picture**	◆ You can include a picture of the user, or the user can add it later.
◆ **Time Zone**	◆ Make sure the time zone setting is accurate.
◆ **Locale**	◆ Make sure the locale setting matches the user's language preference.
Personal Information	Users normally provide the following information for themselves.
◆ **Job Title**	
◆ **About Me**	
◆ **Email**	
◆ **Phone**	
◆ **Text Messaging Email**	
OK or **Cancel**	◆ Click **OK** to save the user information you have entered, or click **Cancel** to discard your entries.

Viewing and Managing User Properties

Path: Port 8443 ESN Administration Console **Management > Users > drop-down arrow next to the user > User Properties**

Table 22-2 *Using the User Properties dialog*

Field, Option, or Button	Information and/or Action

◆ **Profile** button	◆ You can change any of the following that is not synchronized from an LDAP source:
	  ◆ User ID
	  ◆ Picture
	  ◆ Time Zone
	  ◆ Locale
	  ◆ Job Title
	  ◆ About Me
	  ◆ Email
	  ◆ Phone
	  ◆ Text Messaging Email

Managing Groups

Path: Port 8443 ESN Admin Console**Groups**

 Best Practice: Plan groups in advance and use the following worksheets when working in this dialog:

◆ Worksheet 4 - Users and Groups

Table 22-3 *Using the Groups dialog*

Field, Option, or Button	Information and/or Action
Manage Groups dialog (header row)	
◆ **New** button	◆ Click this to begin adding a new non-LDAP internal group.
◆ **Delete** button	◆ Click this to remove the selected groups from the list.

Field, Option, or Button	Information and/or Action
◆ **More** drop-down	With one or more groups selected, you can choose from the following options: ◆ **Disable File Downloads:** "Web Browser Access—Individual Users and Groups" on page 23 ◆ **Enable File Downloads:** "Web Browser Access—Individual Users and Groups" on page 23 ◆ **Use Default File Download Setting:** "Web Browser Access—Individual Users and Groups" on page 23 ◆ **Disable Web Access:** "Web Browser Access—Individual Users and Groups" on page 23 ◆ **Enable Web Access:** "Web Browser Access—Individual Users and Groups" on page 23 ◆ **Use Default Web Access Setting:** "Web Browser Access—Individual Users and Groups" on page 23 ◆ **Desktop Application Settings...:** "Desktop Access—Individual Users and Groups" on page 17 ◆ **Mobile Application Settings...:** "Mobile Device Access—Individual Users and Groups" on page 20 ◆ **Add Administrator Rights:** Lets you assign selected group members as Designated Administrators. ◆ **Remove Administrator Rights:** Lets you remove Direct-administration rights from selected groups.
◆ **Filter List** field	◆ Begin typing a name and press enter to filter the list to only those users who match what you have entered.
Manage Groups (below header row)	
◆ **Type** column	◆ Iconx indicate whether the groups are LDAP, non_LDAP internal, LDAP with Direct Admin rights, non-LDAP with Direct Admin rights.
◆ **Title** column	◆ Displays group titles as defined in LDAP or specified when the group was created. LDAP titles cannot be changed in ESN, non-LDAP titles can be changed. ◆ Click this to edit the group, including changing the group title and the membership configuration.
◆ Arrow drop-down column	◆ Provides access to the following settings for the group: ◆ **Web Access** settings: Depending on what has already been configured, you can enable web access for all group members, disable web access for all group members, or specify that the default file downloading settings be used for all group members.
◆ **Name** column	◆ Displays group names as defined in LDAP or specified when the group was created. Group names cannot be changed.
◆ **Admin** column	◆ This indicates whether the group members are allowed Direct administrative responsibilities because of membership in the group.
Add Group dialog	

Field, Option, or Button	Information and/or Action
◆ **Name:** field	◆ Specify a unique name under which the group is to be stored in the ESN database. You can use only alphanumeric characters (a-z, A-Z, 0-9), hyphens (-), and underscores (_).
	◆ Once the group is created, the name cannot be modified.
	◆ By default, after the group is added, this is what appears in lists of ESN groups.
	However, you can specify whether the group Name or Title is displayed when users are selecting groups, for example in the Share dialog, by modifying the name completion settings, see "Name Completion Settings—Managing How Group Names Display in Drop-Down Lists" on page 97.
◆ **Title:** field	◆ Enter a descriptive group title. This string can include any characters that you can type.
	◆ The title can be modified
	◆ You can specify whether the group Name or Title is displayed when users are selecting groups, for example in the Share dialog, by modifying the name completion settings, see "Name Completion Settings—Managing How Group Names Display in Drop-Down Lists" on page 97.
◆ **Description:** box	◆ If desired, include some text that describes the group, such as what the members of this group have in common.
◆ **Group membership is static** option	◆ Static groups are groups whose membership is directly specified and does not change based on LDAP queries.
◆ **Group membership is dynamic** option	◆ Dynamic groups are populated based on LDAP queries made by ESN. Their membership changes as the meta data returned from ESN's LDAP queries changes.
◆ **Edit group membership** button	◆ Click this to configure the type of group you have selected:
OK or **Cancel**	◆ Click **OK** to save the changes you've made in this dialog or **Cancel** to discard your changes.
	◆ Make sure you have edited the group membership. Otherwise your group will have no members.
Static Membership for Group dialog	
Allow external users and groups option	◆ Select this to allow external users and groups to be added to the list.
Users tab	◆ **User field:** Begin typing a user name, then select a listed user to add it to the Membership list.
Groups tab	◆ **Group field:** Begin typing a group name, then select a listed group to add it to the Membership list.
◆ **Remove** button	◆ Click this to remove a selected user or group (depending on which dialog you are in).
Membership list	◆ A list of the users/groups in the static group.
OK or **Cancel**	◆ Click **OK** to save the changes you've made in this dialog or **Cancel** to discard your changes.

Field, Option, or Button	Information and/or Action
Edit Dynamic Membership dialog	
Tips and Caveats	◆ Users must already have existing ESN user accounts in order for them to be added to a ESN group as described in this section. If your LDAP query includes users who are not already ESN users, the users are not added to the ESN group
	◆ When you configure your LDAP connection, you must specify the name of the LDAP attribute that uniquely identifies the user (the value of this attribute never changes). For eDirectory, this value is GUID. For Active Directory, this value is objectGUID. For more information about this attribute, see "Guid attribute:" on page 31.
	◆ The ESN process that creates a dynamic group uses the LDAP configuration settings in ESN to authenticate to the LDAP directory server used to specify the Base DN (below). The credentials that are used are the LDAP server URL, user DN, and password. For more information on how to configure these and other LDAP configuration settings in ESN, see "LDAP Servers and Synchronization" on page 27.
	◆ The Base DN set below must exist in each LDAP source. Otherwise, the membership of the dynamic group might not be updated correctly.
	◆ If your ESN site is configured with multiple LDAP sources and the base DN that you define for the dynamic group exists in each LDAP source, the membership of the dynamic group contains users from each LDAP source that match the dynamic group's filter.
◆ **Current Membership:** button	◆ Click this to open the Dynamic Group Membership windows and view the users that are included in the group based on the current configuration.
◆ **Base DN:**	◆ Use the LDAP browse button to locate the context where you want the search for users to begin.
◆ **LDAP Filter:**	◆ Specify the LDAP filter you want to use for the query. This is required for the search to return any results.
	◆ For an example and more information, see "Filter:" on page 34.
◆ **Search subtree** option	◆ Select this to have the search extended into sub-containers.
◆ **Update group membership during scheduled ldap synchronization** option	◆ You must either select this or perform a manual ldap synchronization before any users are added to the group you are defining.
	◆ If you do not select this option, the group will not be automatically updated when changes occur in your LDAP directory.
◆ **Test ldap query** button	◆ Use this to see whether the configuration you have specified is working.
OK or **Cancel**	◆ Click **OK** to save the changes you've made in this dialog or **Cancel** to discard your changes.
Dynamic Group Membership window	
Users tab	◆ This displays a list of the users and groups that are members of the dynamic group.
◆ **Close** button	◆ Use this to return to the previous window.