

Client Administration

Client Administrators have the ability to manage access privileges to Intellix functions or services through the setup of *users* and *roles*. These functions are available through the **Manage Users** and **Manage Roles** Administration menu items in Intellix. For organizations with multiple Client Administrators, one Client Administrator can create roles and users, and another will need to approve.

For organizations with only one Client Administrator, the single Client Administrator will create roles and users, and they will be automatically approved on Save.

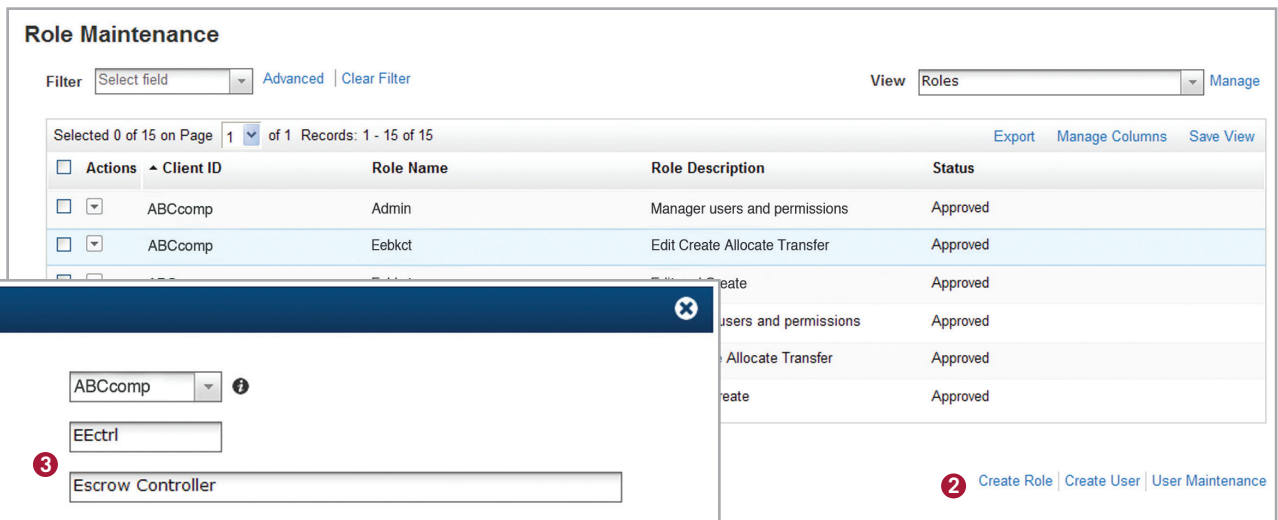
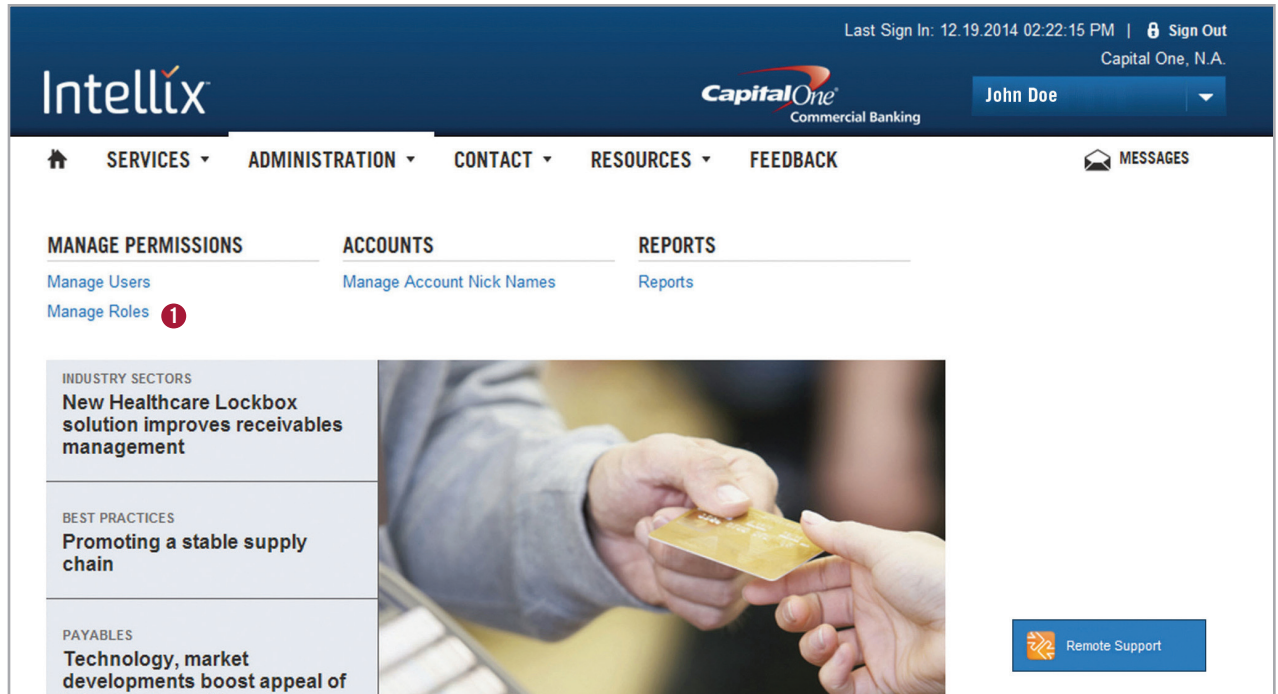
Creating a Role

A Role is a group of permissions to allow users access to specific functions or services in Intellix. Roles need to be setup in order to setup users.

1. Click **Manage Roles** from the *Administration* menu in Intellix. The Role Maintenance screen displays.
2. Click the **Create Role** link from the bottom right corner.

NOTE: For this example, we will create a role for a Controller. This role will have access to all Escrow Express permissions.

3. Enter a short **Role Name** (up to 8 characters) and a meaningful **Role Description** (up to 30 characters).
4. Click **Save and Continue**.



Creating a Role (continued)

Services and functions that your organization is entitled to displays within tabs. Each service or function has its own tab. In the example to the right, the organization is entitled to Escrow Express, Admin and Remote Deposit.

5. Assign permissions by selecting the appropriate tabs and permission checkboxes and/or radio buttons.

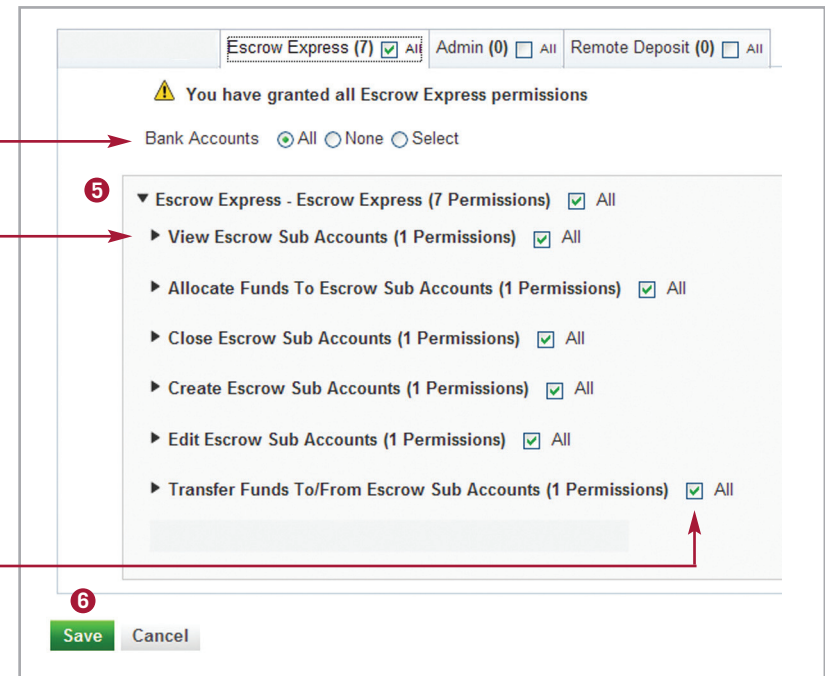
NOTE:

- Selecting the **All** checkbox on a tab will select all permissions on that tab.
- By selecting the **All** radio button for a data permission within a tab, such as Accounts on the Escrow Express tab, the role will have access to all of that data; and if a new data item is added in the future, the role will automatically have access to that data.
- To select individual permissions, select the triangle next to a permission name and then select the individual permissions.
- Select **All** check for a permission group to grant **All** permissions in that group.

6. Click **Save** in the lower left corner.

If your organization has more than one approver, the role will be in an “Entered” status once you click **Save**. This means that the role will need to be approved by a different Client Administrator; make sure to notify another Administrator in your organization to approve. If you are the sole Client Administrator for your organization, clicking **Save** automatically approves the role.

NOTE: This guide includes the steps for creating roles and users, and for using Administration Reports. Please refer to the Specific Permissions guides available on Intellix to review specific Service Permissions.



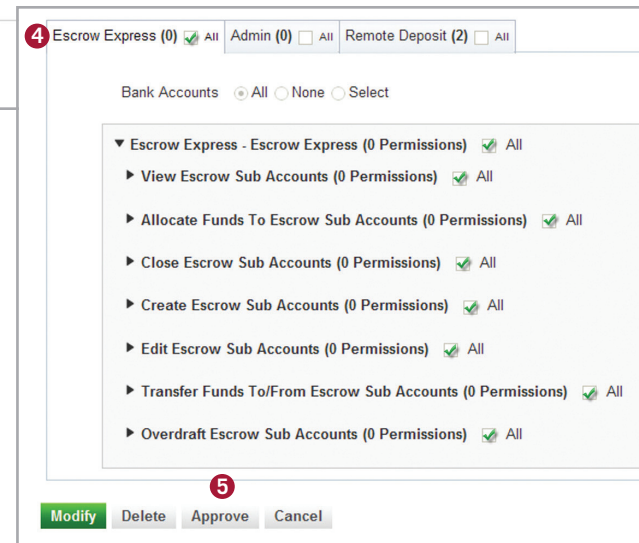
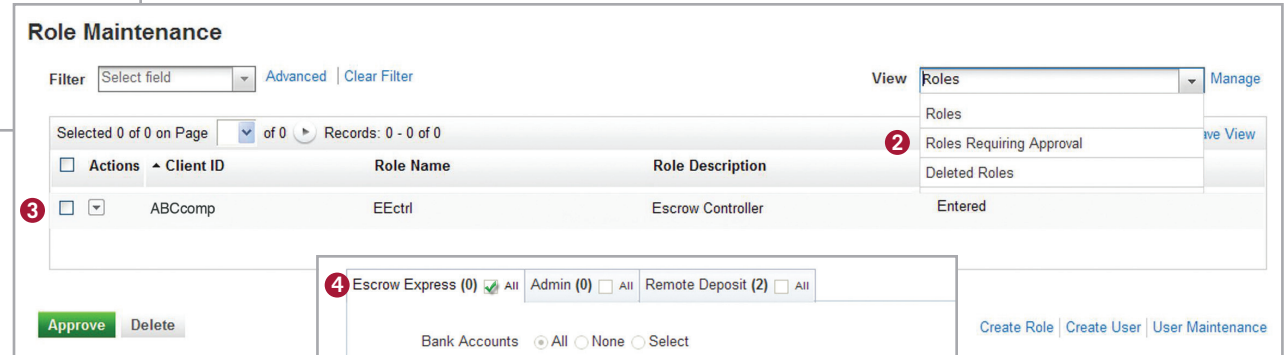
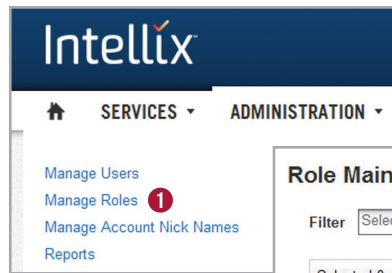
NOTE: This screen capture illustrates the Escrow Express data and functional permissions. Permissions for other services will vary (e.g. some services do not have the Bank Accounts data permission available).

Approving Roles

If your organization has more than one Client Administrator, any newly created role will need to be approved by a different Client Administrator.

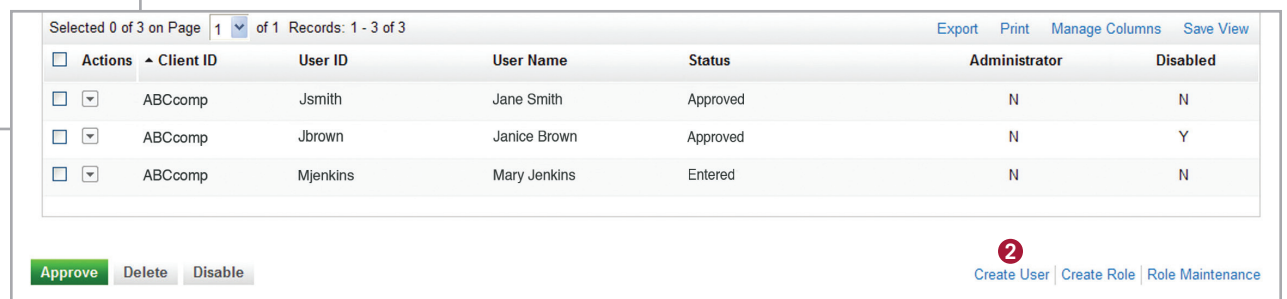
1. Select **Manage Roles** from the *Administration* menu in Intellix. The *Role Maintenance* screen will display, showing a list of approved roles in your organization and roles awaiting approval.
2. From the **View** drop-down, select **Roles Requiring Approval**.
3. Click the role. The *Role Detail* screen displays.
4. Review the role information and permissions assigned.
5. Click **Approve**.

Note: You can approve one or more roles from the *Role Maintenance* screen by selecting the checkbox for the role(s) and clicking **Approve**.



Creating Users

1. Select **Manage Users** from the *Administration* menu in Intellix.
2. Click the **Create User** link in bottom right.



Creating Users (continued)

3. Complete the **User Information**:

- **User Name:** User's first and last name.
- **User ID:** The user will use this ID to log into Intellix. The User ID must be between 6 and 18 characters, contain at least one number, one letter and have no special characters.
- **Locale and Time Zone:** Will automatically populate to the ET time zone.
- **Email Address:** Enter the user's valid email address.
- **Set as Administrator:** This function will only be visible to organizations that have elected to have a single administrator who can create and approve in a single step. If this is applicable in your organization, and you need to create another "Single Administrator," select Yes and make sure to assign the proper Admin role(s) to create and approve users and roles.

- **Authentication Method:** Intellix provides multiple layers of security, including the use of soft token software on a mobile device. One of the following Authentication Methods must be selected:
 - Soft Token on Mobile Device
 - Hard Token

NOTE:

- For users who choose soft token on a mobile device, advise the user to download the RSA SecurID app on their mobile device
- For users who choose hard token, contact Treasury Management Client Services at 866-632-8888
- **Industry:** Your organization's industry classification will be used to send you content and information via Lead Reports on Intellix that are relevant to your business.
- **Address, City, State, Country and Zip Code:** User's work address.
- **Phone Number:** The best number to reach the user,
- **Personal Verification Code:** This code will be saved in the user's Intellix Profile. The user will be requested to provide this code to verify their identity and to access their first time credentials which will be sent to them via email. This code must be between 8 and 30 characters, contain at least one number, one letter and no special characters.
NOTE: Make sure the user knows this case-sensitive code for retrieval of their first-time Intellix login credentials.

4. Click **Save**.

User Maintenance

3 User Information

Client ID *	ABCcomp	Locale *	English (United States)
User Name *	Janice Brown	Timezone *	EST US/Eastern
User ID *	jbrown	Email Address *	JaniceBrown@abccompany.com
Set As Administrator	<input type="radio"/> No <input type="radio"/> Yes	User Disabled Status	<input type="checkbox"/>

4 Additional Information

Disable Description	
Authentication Method *	Soft Token on Mobile Device
Industry *	Professional Services
Address Line 1 *	123 Main st
Address Line 2	
Address Line 3	
City *	New York
State *	NEW YORK
Province	
Country *	UNITED STATES
Zip Code *	10001
Phone Number *	631-123-4567
Personal Verification Code *	Code1234

4 Save Reset Cancel

Creating Users (continued)

5. If your organization has Remote Deposit services expand the RDC group to assign the **RDC Location** they will work from. If the user needs access to more than one location, select “None”. In the near future, this choice will display as “All”.

6. A Role Assignment section displays. You can assign roles in three different ways.

A. Copy An Existing User: Copy the same roles assigned to an existing user

B. Assigning Existing Roles: Assign roles by selecting them for the user

C. Create and Assign New Role: Create a new role and assign it to the user

7. Click **Save**.

If your organization has more than one approver, the user will be in an “Entered” status once you click **Save**. This means that the user will need to be approved by a different Client Administrator. Make sure to notify another Administrator in your organization to approve. If you are the sole Administrator for your organization, clicking **Save** automatically approves the user.

NOTE: Entitling a user to a Remote Deposit location can only be done directly on the user’s profile.

User Maintenance

— User Information for Janice Brown — User Status: Entered ⚠

Client ID*	<input type="text" value="ABCcomp"/>	Locale*	<input type="text" value="English (United States)"/>
User Name*	<input type="text" value="Janice Brown"/>	Timezone*	<input type="text" value="EST US/Eastern"/>
User ID*	<input type="text" value="Jbrown"/>	Email Address*	<input type="text" value="Jbrown@ABCcompany.com"/>
		User Disabled Status	<input type="checkbox"/>

Set As Administrator ⓘ

No
 Yes

— Additional Information —

— Remote Deposit —

RDC Location 5

6

A **Copy an Existing User**
View and copy an existing user's accounts and permissions.

Jane Smith-Jsmith

John Jones-Jjones

Mary Jenkins-Mjenkins

Robert Miller-Rmiller

B **Assign Existing Roles**
Entitle this user with a predefined role of accounts and permissions, or you can **Create and Assign New Role** C

Admin

EEbkct

EEbkpr

EEctrl

EEmgt

Escrow

- or -

7

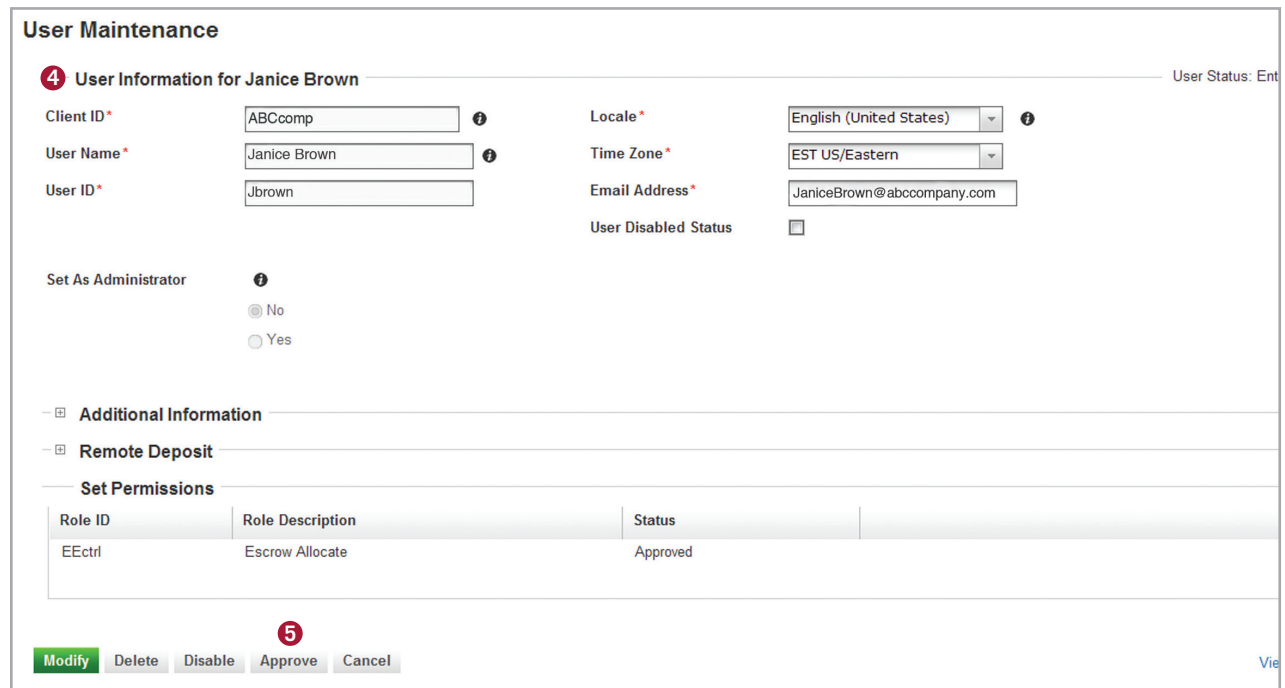
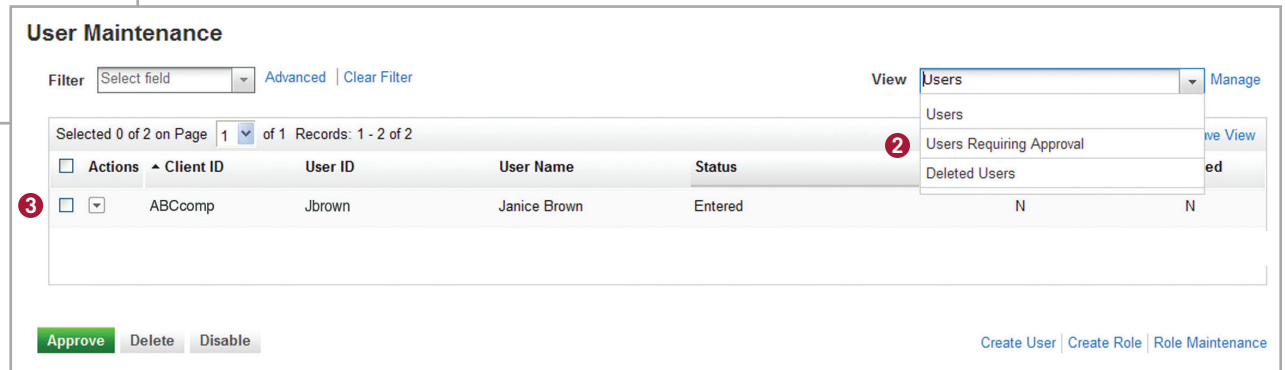
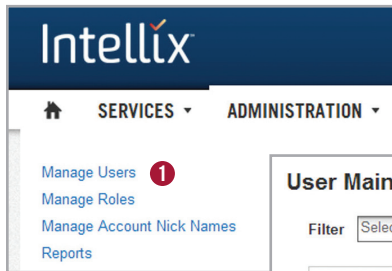
[View Audit](#)

Approving Users

If your organization has more than one Client Administrator, any newly created user will need to be approved by a different Client Administrator.

1. Select **Manage Users** from the *Administration* menu in Intellix. The *User Maintenance* screen will display, showing a list of all users in your organization with access or awaiting access to Intellix.
2. From the **View** drop-down, select **Users Requiring Approval**.
3. Click the User. The *User Detail* screen displays.
4. Review the user information and role(s) assigned.
5. Click **Approve**.

Note: You can approve one or more users from the *User Maintenance* screen by selecting the check-box for the user(s) and clicking Approve.



Viewing Administration Reports

1. Select **Reports** from the *Administration* menu.

The following four Administrative reports will display:

- **Intellix Approved User Permissions:**

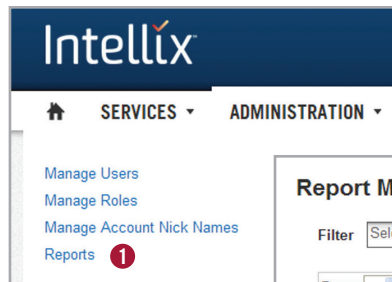
Reflects users for that organization and their assigned roles/permissions.

- **Intellix Audit:** This report includes user login activity into Intellix and user activity in Client Administration. Audit activity for services such as Remote Deposit and Capital One Escrow Express can be accessed within reports for those services.

- **Intellix Client Detail:** Reflects client level entitlements.

- **Intellix Roles:** Reflects the roles that exist for the organization.

2. Click a report to view; some reports, such as Intellix Audit and Intellix Roles, will prompt you to first select filter criteria to view the report.

A screenshot of the 'Report Management' interface. At the top, there is a 'Filter' dropdown menu with 'Select field' and a 'Clear Filter' button. To the right, there is a 'View' dropdown menu with 'All Reports' selected. Below this, there is a table with the following columns: 'Actions', 'Report Name', 'Filter Name', 'Report Group', and 'Platform Services'. The table contains four rows of reports. The first row is 'Intellix Approved User Permissions' with a red circle containing the number '2' next to its dropdown arrow. The other rows are 'Intellix Audit', 'Intellix Client Detail', and 'Intellix Roles'. To the right of the table, there is a 'View' dropdown menu with 'All Reports' selected. Below the table, there are four more options: 'All Reports', 'All Saved Filters', 'Admin Reports', and 'Platform Services'.

Actions	Report Name	Filter Name	Report Group	Platform Services
2	Intellix Approved User Permissions		Admin	
	Intellix Audit		Admin	Platform Services
	Intellix Client Detail		Admin	Platform Services
	Intellix Roles		Admin	Platform Services