

Module Migration

Published: 2023-07-22

The ExtraHop system now offers separate modules with features segmented and optimized for security and performance use cases.

The Network Detection and Response (NDR) module provides security and investigation workflows, and the Network Performance Management (NPM) module provides operations and performance workflows. Additional modules are available for Packet Forensics and Intrusion Detection Systems. Learn more about [modules](#).

This guide provides information about [global system changes](#), [administrative tasks](#), and guidelines about which [features](#) are available for each module.

Global system changes

The ExtraHop system automatically updates certain features as part of the module migration.

Default Login Page

For users with NPM access, the default dashboard page that displays after login can be specified by an administrator.

For NPM users, the default [dashboard](#) page that displays after login can be specified [globally by an administrator](#) or be personally set by a user. If no dashboard is specified, the [Active Directory dashboard](#) appears.

Users can navigate to their preferred default dashboard, click on the command menu in the upper right corner of the page, and select Set as Default Dashboard.

Tuning Rules

The system will remove the All Detection Types option from the Detection Type criteria for tuning rules.

[Tuning rules](#) are displayed based on the module access options specified by [user privileges](#).

Existing tuning rules that contain the All Detection Types criteria are automatically split into two rules that are specific to either security or performance categories. The existing rule is modified to specify All Security Detection Types, and a new rule is created for All Performance Detection Types. During migration, hidden detections might be associated with a new tuning rule that matches the detection criteria.

When you create or edit a tuning rule, you can specify Detection Type criteria depending on your module access privileges. The Detection Type dropdown can include options for All Security Detection Types or All Performance Detection Types.

Notification Rules

Detection notification rules no longer support criteria that apply to both security and performance detections. Notification rules are displayed based on your module access privileges.

[Detection notification rules](#) that specify the Detection event type are automatically split into two rules that are specific to either security or performance categories. The existing rule is modified to specify the new Security Detection event type and includes only the security criteria from the original rule. A new rule is created for the new Performance Detection event type and includes only the performance criteria from the original rule.

When a notification rule is split during migration, detection types that are associated with both security and performance are only included in the security version of the rule to avoid duplicate notifications.

Disabled notification rules that contain both security and performance criteria are not split. The rule converts to a security only rule and remains disabled.

Actions specified by notification rules, such as email distribution lists and webhooks, are included in the modified NDR rule and the new NPM rule. Review these actions to ensure security and performance notifications are sent to the correct audience.

When you create a notification rule, you can specify either Security Detection or Performance Detection event types, depending on the module access options specified in your [user privileges](#). After you have selected an event type, you are only able to add detection type and category criteria associated with the selected event type.

Administrative Tasks

Migrated systems grant all users access to both Network Performance Monitoring (NPM) and Network Detection and Response (NDR) modules.

Administrators must grant role-based access for all users who log in through [remote authentication](#) (LDAP, RADIUS, SAML, and TACACS+) as well as [local users](#).

There are two sets of [user privileges](#) that must be granted:

Module Access

These user privileges determine which features a user can access. For example, a user must be granted full access to the NDR module to see attack detections. See [features specific to each module](#).

System Access

These user privilege levels determine the level of functionality users have with module features. For example, full write users can create and edit all system objects.

The following sections provide instructions on how to update user privileges.

Updating remote authentication settings

Administrators must review remote authentication settings for the NDR and NPM modules and update if necessary.

Network Detection and Response (NDR) module access

Remote authentication settings for NDR module access must be configured on [Reveal\(x\) Enterprise](#) systems where the now deprecated Detections Access global privilege policy was not previously enabled.

User access to the NDR module is inherited directly from the Detections Access global privilege policy setting. For example, if only specific users were granted detections access with full write system access before migration, those same users now have NDR module access with full write system privileges after migration.

Network Performance and Monitoring (NPM) module access

Remote authentication settings for NPM module access must be configured on both [Reveal\(x\) 360](#) and [Reveal\(x\) Enterprise](#) systems.

Update the custom IdP configuration in Reveal(x) 360

Update your custom Identity Provider (IdP) configuration in Reveal(x) 360 to grant user privileges for NDR and NPM module access.

Remote authentication for NDR module access

NDR module access is automatically configured with the previous settings for Detections Access Control.

Remote authentication for NPM module access

You must update your custom Identity Provider (IdP) configuration to grant users access to the NPM module in Reveal(x) 360.

Add NPM privileges to the ExtraHop application in your identity provider


If your IdP does not include a group attribute for the ExtraHop application, you must add a user attribute and name to match what you will configure in Reveal(x) 360.

1. Log in to your identity provider.
2. Add an attribute name and value.
3. Save the configuration.

Next steps

Learn more about configuring [Okta](#), [Google](#), [Azure AD](#) or [Jumpcloud](#).

Add NPM privileges to your identity provider settings in Reveal(x) 360

1. Log in to the Reveal(x) 360 system with an account that has System and Access Administration privileges.
2. Click the System Settings icon  and then click **User Access**.
An Action Required panel will guide you through the remaining configuration steps. If the Action Required panel does not appear, you do not need to update your IdP settings.
3. Enter a name in the Attribute Name field.
4. Enter a name in the Attribute Value field.



Note: The attribute name and value must match the settings configured on your IdP.

5. Select the checkbox to confirm that you are ready to begin the update.



Important: All users will be logged out of the system after you click **Update Now** in the next step.


6. Click **Update Now**.

Update the custom IdP configuration in Reveal(x) Enterprise

Update your custom Identity Provider (IdP) configuration in Reveal(x) Enterprise to grant user privileges for NDR and NPM module access.

Remote authentication for NPM module access

You must update your custom Identity Provider (IdP) configuration to grant users access to the NPM module in Reveal(x) Enterprise.

1. Log in to the Reveal(x) Enterprise console with an account that has System and Access Administration privileges.
2. Click the System Settings icon  and then click **All Administration**.
3. In the Access Settings section, click **Global Policies**.
An Action Required panel displays a link to view your remote authentication settings. If the Action Required panel does not appear, you do not need to update your IdP settings.
4. Click **View Remote Authentication**.
5. Select your authentication method from the **Remote authentication method** dropdown.
6. Complete the following steps for the remote authentication method you selected:

Option

Description

LDAP


Configure NPM module access based on your privilege assignment option.

1. Obtain privileges level from remote server:

Option	Description
	<ol style="list-style-type: none"> 1. Enter a distinguished name in the NPM Module Access DN field. 2. Remote users have full write access <ol style="list-style-type: none"> a. Select Full access. 3. Remote users have full read-only access <ol style="list-style-type: none"> a. Select Full access.
RADIUS	<p>Configure NPM module access based on your privilege assignment option.</p> <ol style="list-style-type: none"> 1. Remote users have full write access <ol style="list-style-type: none"> a. Select Full access. 2. Remote users have full read-only access <ol style="list-style-type: none"> a. Select Full access.
SAML	<p>Edit the identity provider settings to add an attribute name and attribute value for NPM module access. The attribute name and values must match the values configured in your identity provider.</p>
TACACS+	<p>Configure NPM module access based on your privilege assignment option.</p> <ol style="list-style-type: none"> 1. Obtain privileges level from remote server: <ol style="list-style-type: none"> 1. On your TACACS+ server, add the following custom attribute: Attribute: <code>npmfull</code> Value: 1 2. Remote users have full write access <ol style="list-style-type: none"> a. Select Full access. 3. Remote users have full read-only access <ol style="list-style-type: none"> a. Select Full access.

7. Return to the Global Policies page.

8. Select the checkbox to confirm that you are ready to start the update.


 **Important:** All users will be logged out of the system except for the setup user account.

9. Click **Update Now**.

Remote authentication for NDR module access


If your Reveal(x) Enterprise system had Detection Access Control enabled as a global policy prior to migration, NDR module access is automatically configured with the previous settings for Detections Access Control.

If Detection Access Control was not enabled, you must update your custom Identity Provider (IdP) configuration to grant users access to the NDR module in Reveal(x) Enterprise.

1. Log in to the Reveal(x) Enterprise console with an account that has System and Access Administration privileges.
2. Click the System Settings icon  and then click **All Administration**.

3. In the Access Settings section, click **Global Policies**.
An Action Required panel displays a link to view your remote authentication settings. If the Action Required panel does not appear, you do not need to update your IdP settings.
4. Click **View Remote Authentication**.
5. Select your authentication method from the **Remote authentication method** dropdown.
6. Complete the following steps for the remote authentication method you selected:


Option	Description
LDAP	<p>Configure NDR module access based on your privilege assignment option.</p> <ol style="list-style-type: none"> 1. Obtain privileges level from remote server: <ol style="list-style-type: none"> 1. Enter a distinguished name in the NDR Module Access DN field. 2. Remote users have full write access <ol style="list-style-type: none"> a. Select Full access. 3. Remote users have full read-only access <ol style="list-style-type: none"> a. Select Full access.
RADIUS	<p>Configure NDR module access based on your privilege assignment option.</p> <ol style="list-style-type: none"> 1. Remote users have full write access <ol style="list-style-type: none"> a. Select Full access. 2. Remote users have full read-only access <ol style="list-style-type: none"> a. Select Full access.
SAML	<p>Edit the identity provider settings to add an attribute name and attribute value for NDR module access. The attribute name and values must match the values configured in your identity provider.</p>
TACACS+	<p>Configure NDR module access based on your privilege assignment option.</p> <ol style="list-style-type: none"> 1. Obtain privileges level from remote server: <ol style="list-style-type: none"> 1. On your TACACS+ server, add the following custom attribute: Attribute: <code>ndrfull</code> Value: <code>1</code> 2. Remote users have full write access <ol style="list-style-type: none"> a. Select Full access. 3. Remote users have full read-only access <ol style="list-style-type: none"> a. Select Full access.

7. Return to the Global Policies page.
8. Select the checkbox to confirm that you are ready to start the update.
 -  **Important:** All users will be logged out of the system except for the setup user account.
9. Click **Update Now**.

Updating local user settings

Administrators must review local user access privileges for the NDR and NPM modules and update if necessary.

Update local users in Reveal(x) 360

1. Log in to Reveal(x) 360, click the System Settings icon , and then click **All Administration**.
2. Click **User Access**.
3. In the Users section, click **View Users**.
4. Click a user to view and modify access privileges.

Identity Provider
ExtraHop

System Access

System and access administration

System administration

Full write

Limited write

Personal write

Full read-only

Restricted read-only

NDR Module Access

Full access

No access

NPM Module Access

Full access

No access

Packet and Session Key Access

Packets and session keys

Packets only

Packet slices only

No access

Update local users in Reveal(x) Enterprise

1. Log in to the Administration settings on the ExtraHop system through <https://<extrahop-hostname-or-IP-address>/admin>.
2. In the Access Settings section, click **Users**.
3. Click a user to view and modify access privileges.

User Privileges

System and access administration [?](#)

Limited privileges [?](#)

System Access <input type="radio"/> Full write ? <input checked="" type="radio"/> Limited write ? <input type="radio"/> Personal write ? <input type="radio"/> Full read-only ? <input type="radio"/> Restricted read-only ? <input type="radio"/> No privileges ?	NDR Module Access <input checked="" type="radio"/> Full access ? <input type="radio"/> No access	NPM Module Access <input type="radio"/> Full access ? <input checked="" type="radio"/> No access	Packet and Session Key Access <input type="radio"/> Packets and session keys ? <input type="radio"/> Packets only ? <input type="radio"/> Packet slices only ? <input checked="" type="radio"/> No access
---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Features available by module

The table below shows the major features that are available by module. Features that are not listed are available in both modules.

Feature	NDR	NPM
Security Overview page	Y	N
Executive Reports	Y	N
Built-in Security Dashboards	Y	N
Security detections	Y	N
MITRE map	Y	N
Investigations	Y	N
Tuning rules for security detections	Y	N
Notification rules for security detections and threat briefings	Y	N
Threat Briefings	Y	N
Threat Intelligence	Y	N
Custom Dashboards	N	Y
Built-in Performance Dashboards	N	Y
Performance detections	N	Y
Tuning rules for performance detections	N	Y
Notification rules for performance detections	N	Y
Alerts	N	Y