AD FS AUTHENTICATION POLICIES

SERVER 2012R2

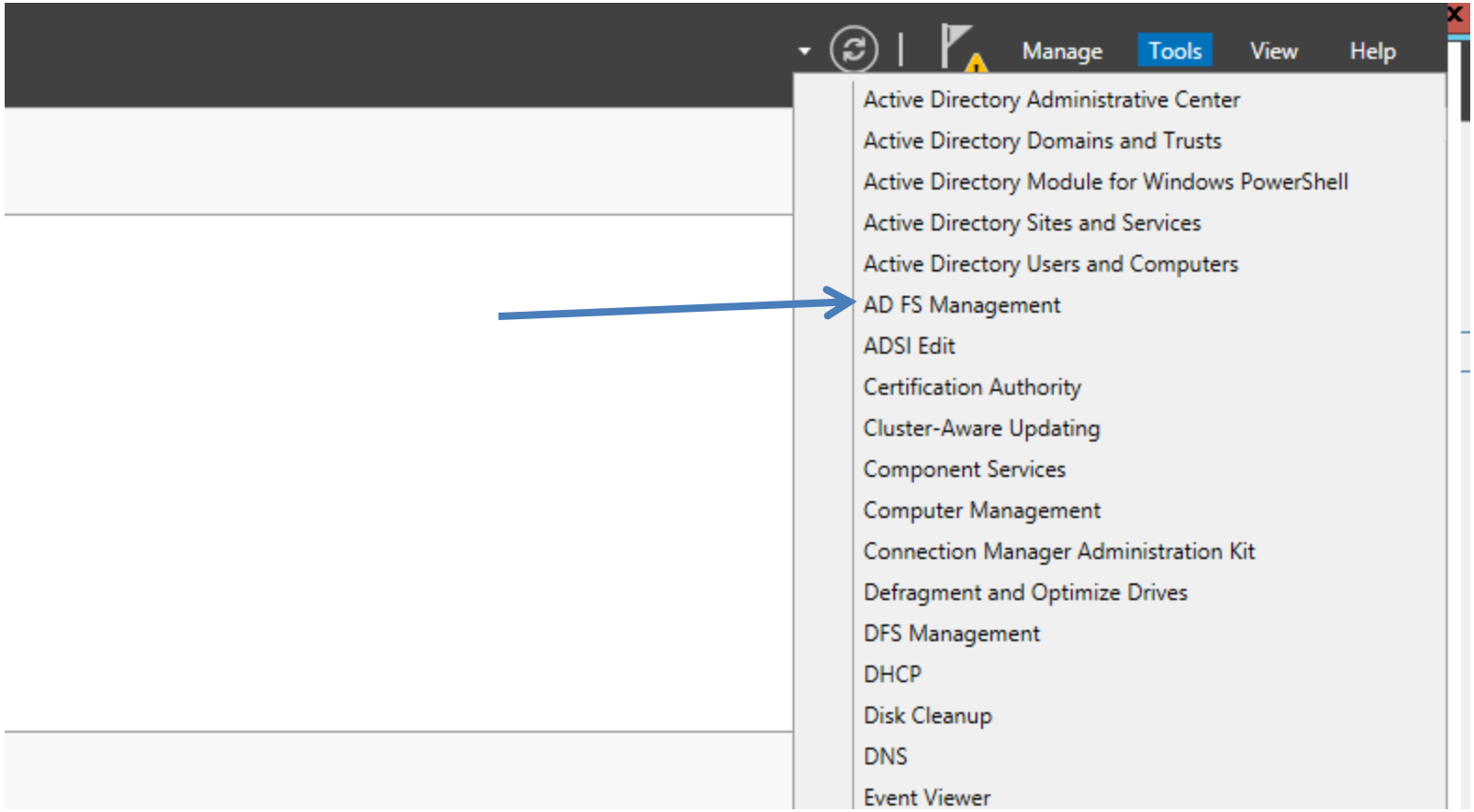
CONFIGURE PRIMARY AUTHENTICATION GLOBALLY

- In AD FS in Windows Server 2012 R2, you can specify an authentication policy at a **global scope** that is applicable to all applications and services that are secured by AD FS.

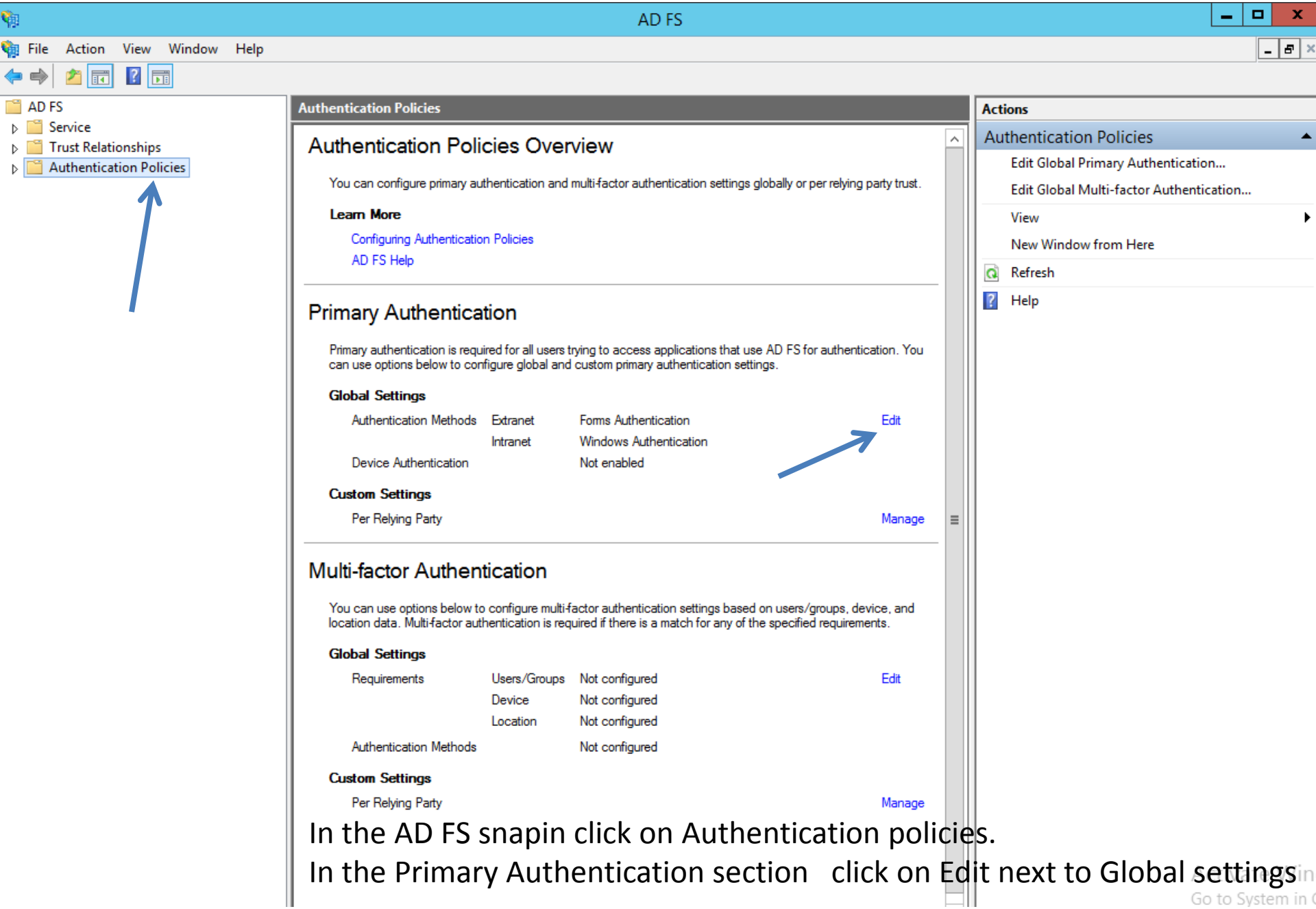
- You can also set authentication policies for specific applications and services that rely on party trusts and are secured by AD FS.

- Specifying an authentication policy for a particular application per relying party trust does not override the global authentication policy. If either global or per relying party trust authentication policy requires MFA, MFA is triggered when the user tries to authenticate to this relying party trust.

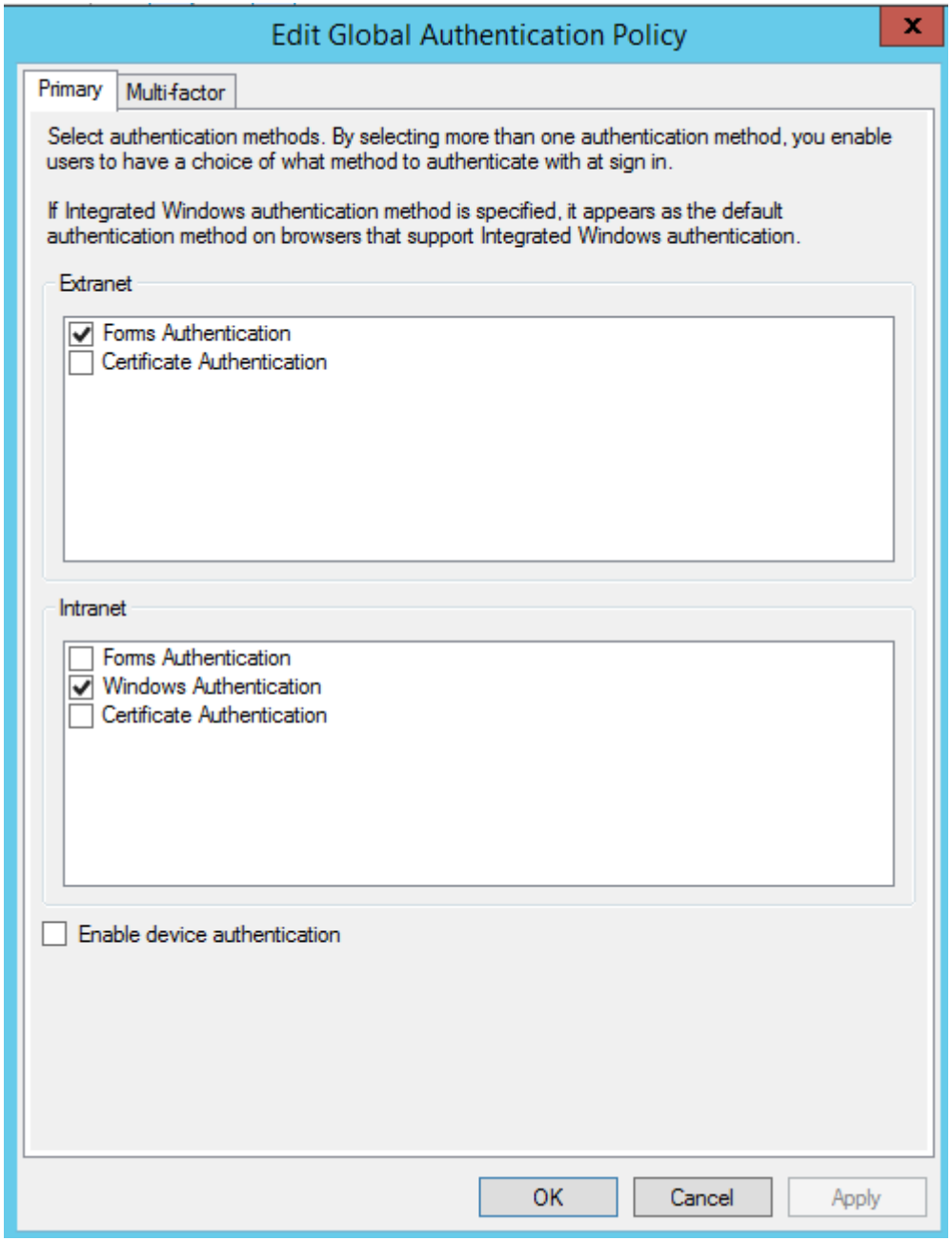
- The global authentication policy is a fallback for relying party trusts for applications and services that do not have a specific configured authentication policy.



Click on Tools AD FS Management



In the AD FS snapin click on Authentication policies.
In the Primary Authentication section click on Edit next to Global settings

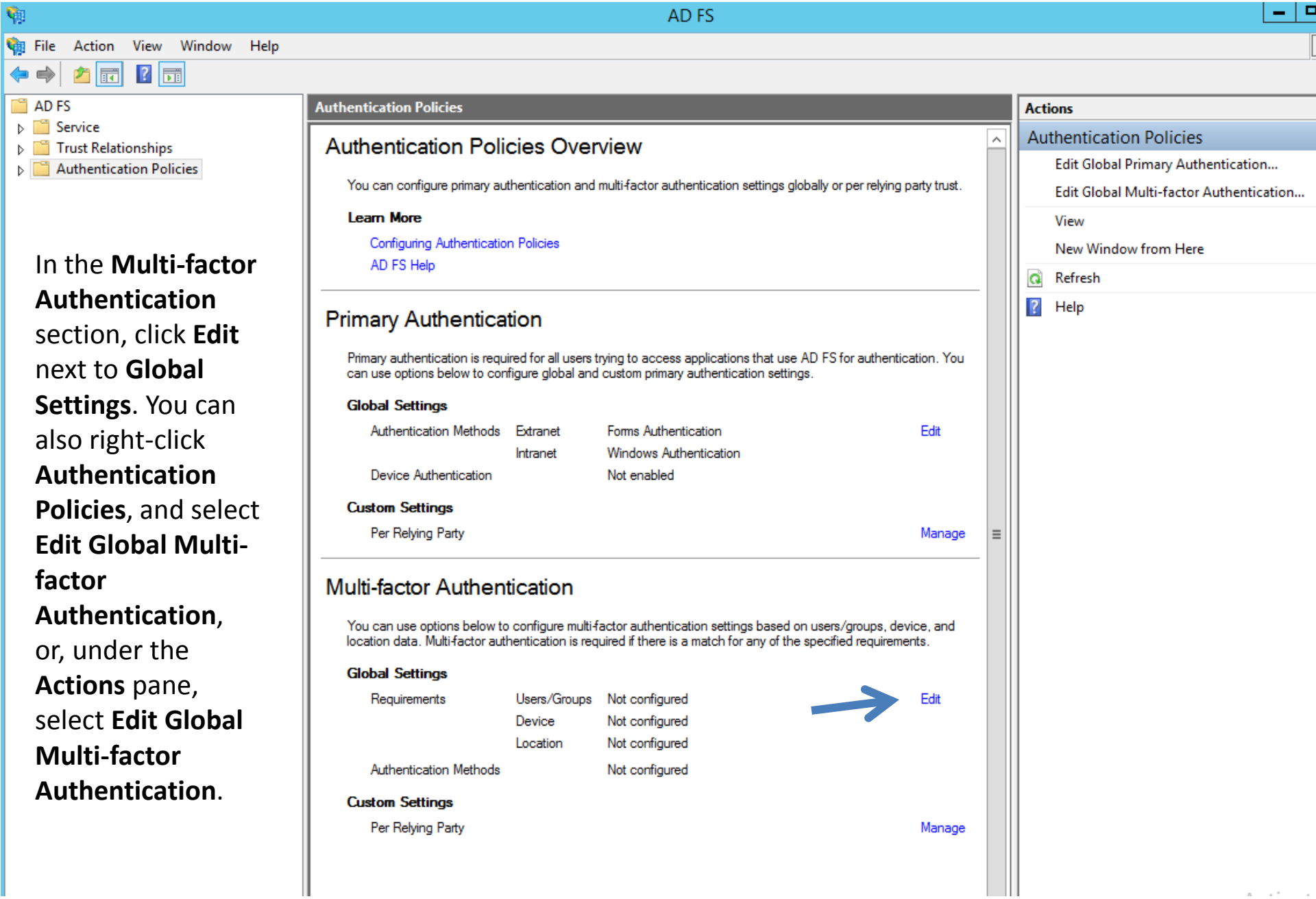


In the **Edit Global Authentication Policy** window, on the **Primary** tab, you can configure the following settings as part of the global authentication policy:

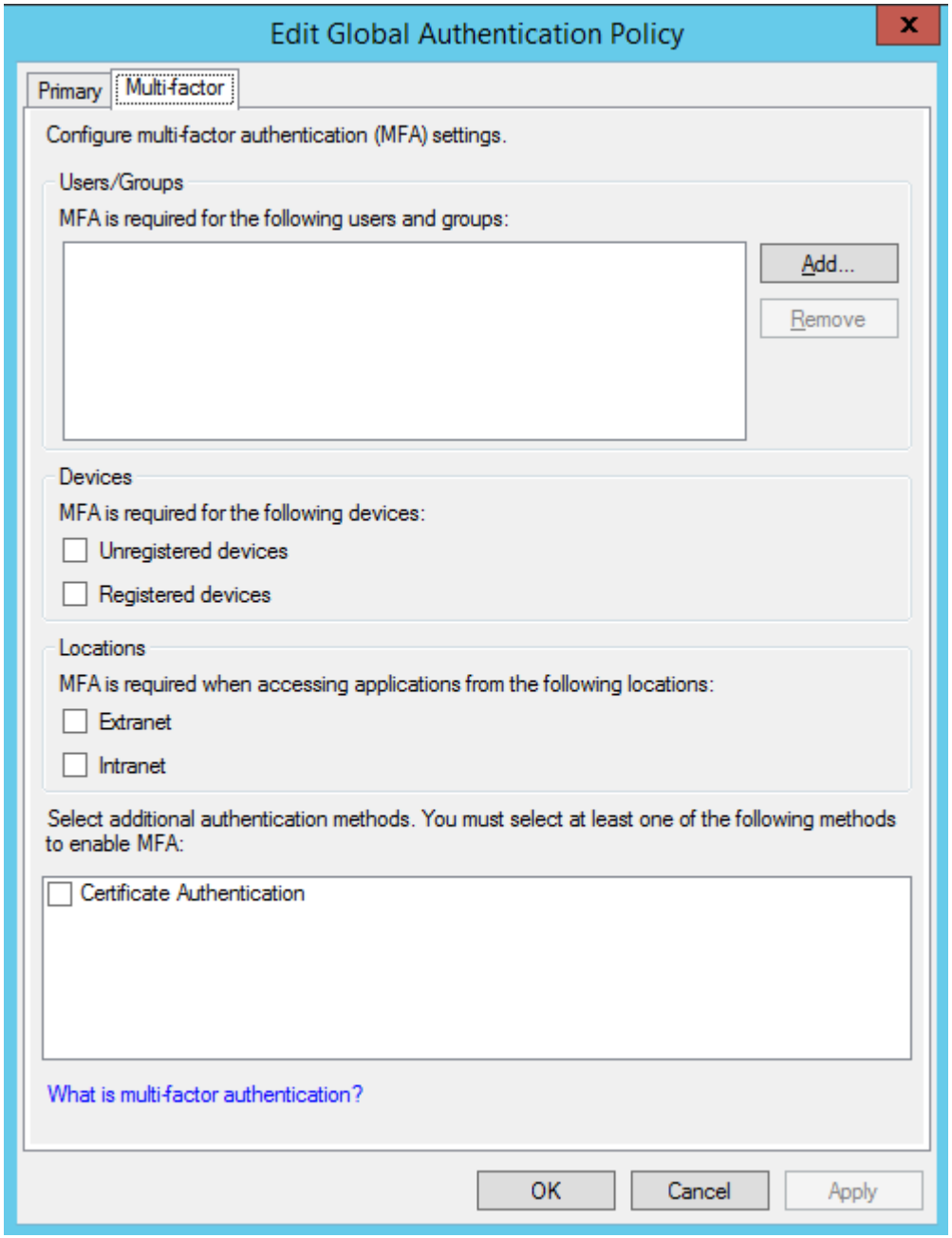
- Authentication methods to be used for primary authentication. You can select available authentication methods under the **Extranet** and **Intranet**.

Device authentication via the **Enable device authentication** check box.

CONFIGURE PRIMARY AUTHENTICATION PER RELYING PARTY TRUST



In the **Multi-factor Authentication** section, click **Edit** next to **Global Settings**. You can also right-click **Authentication Policies**, and select **Edit Global Multi-factor Authentication**, or, under the **Actions** pane, select **Edit Global Multi-factor Authentication**.

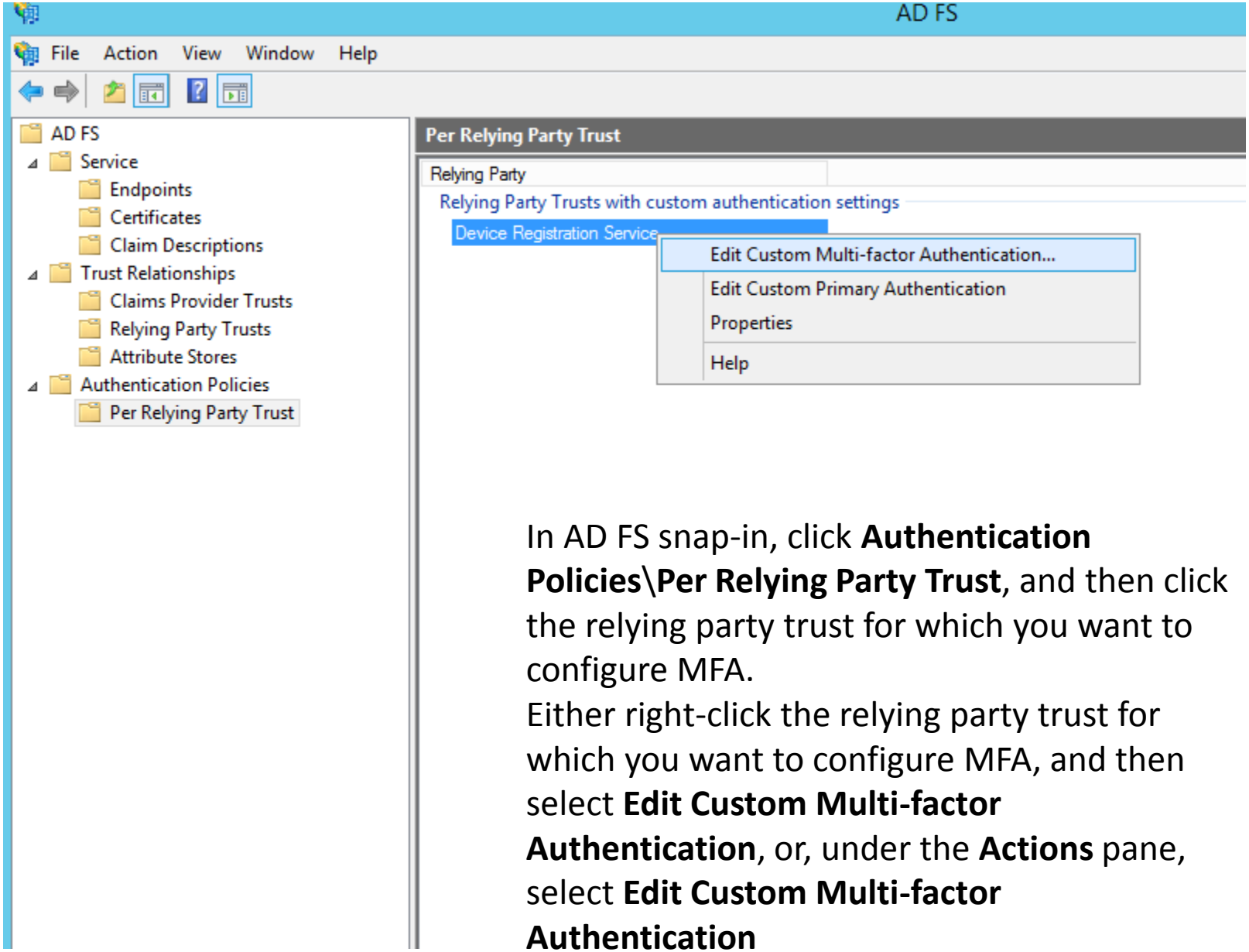


In the **Edit Global Authentication Policy** window, under the **Multi-factor** tab, you can configure the following settings as part of the global multi-factor authentication policy:

Settings or conditions for MFA via available options under the **Users/Groups**, **Devices**, and **Locations** sections.

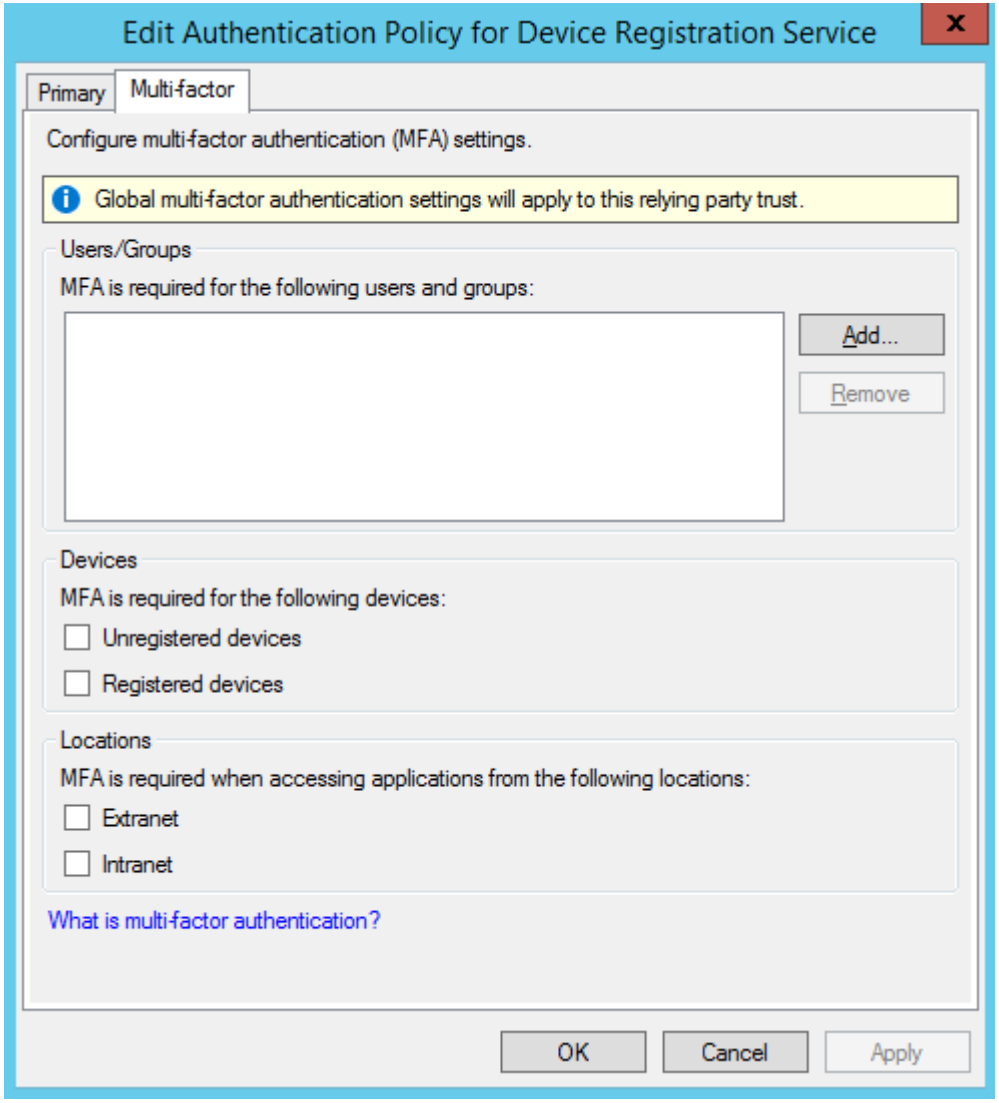
To enable MFA for any of these settings, you must select at least one additional authentication method. **Certificate Authentication** is the default available option. You can also configure other custom additional authentication methods, for example, Windows Azure Active Authentication

CONFIGURE MULTI-FACTOR AUTHENTICATION PER RELYING PARTY TRUST



In AD FS snap-in, click **Authentication Policies\Per Relying Party Trust**, and then click the relying party trust for which you want to configure MFA.

Either right-click the relying party trust for which you want to configure MFA, and then select **Edit Custom Multi-factor Authentication**, or, under the **Actions** pane, select **Edit Custom Multi-factor Authentication**



In the **Edit Authentication Policy for <relying_party_trust_name>** window, under the **Multi-factor** tab, you can configure the following settings as part of the per-relying party trust authentication policy:

- Settings or conditions for MFA via available options under the **Users/Groups**, **Devices**, and **Locations** sections.