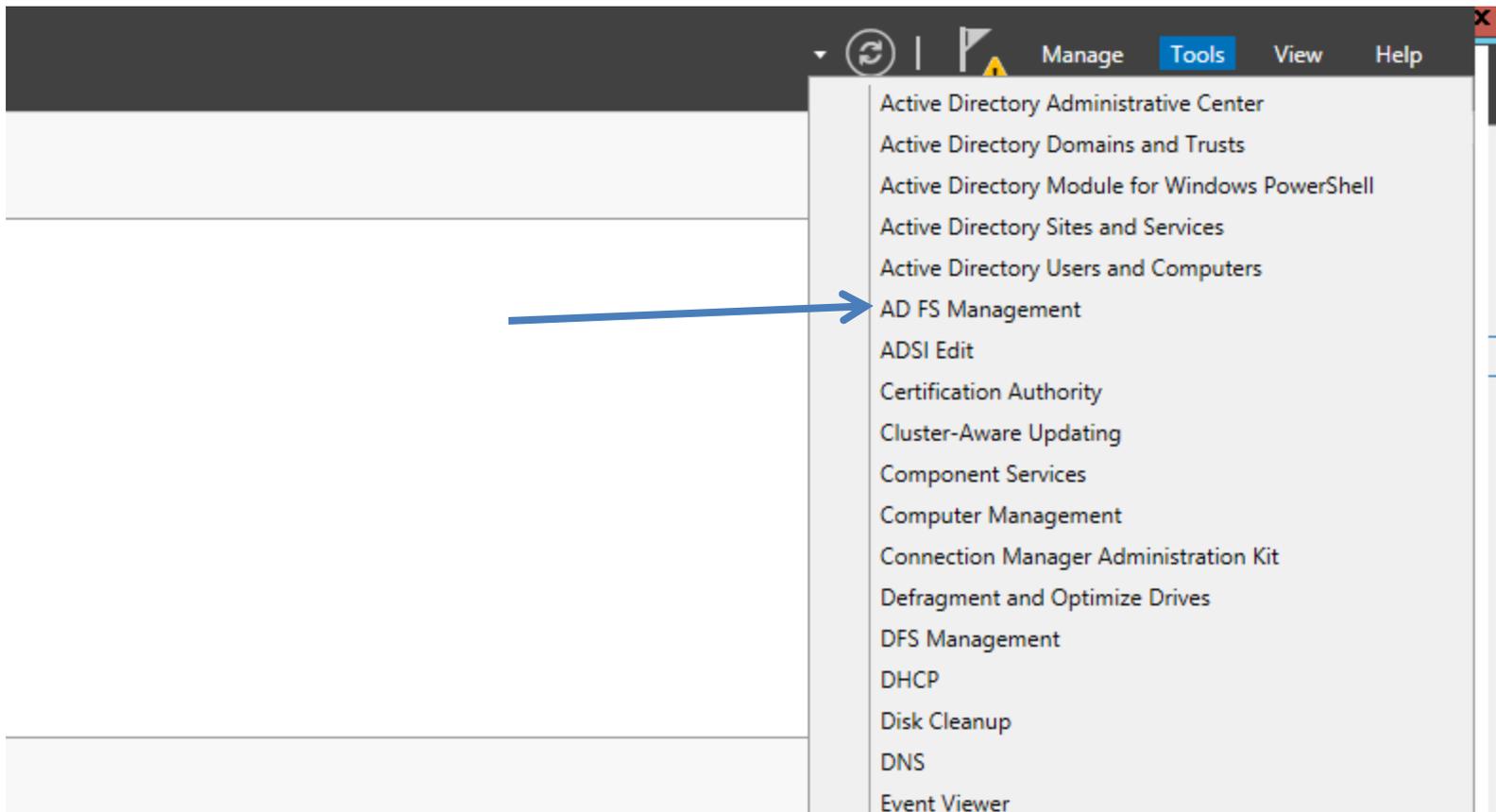


# AD FS AUTHENTICATION POLICIES

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

AD FS

File Action View Window Help

AD FS

- Service
- Trust Relationships
- Authentication Policies

### Authentication Policies Overview

You can configure primary authentication and multi-factor authentication settings globally or per relying party trust.

**Learn More**

- [Configuring Authentication Policies](#)
- [AD FS Help](#)

### Primary Authentication

Primary authentication is required for all users trying to access applications that use AD FS for authentication. You can use options below to configure global and custom primary authentication settings.

**Global Settings**

Authentication Methods	Extranet	Forms Authentication	<a href="#">Edit</a>
	Intranet	Windows Authentication	
Device Authentication		Not enabled	

**Custom Settings**

Per Relying Party	<a href="#">Manage</a>
-------------------	------------------------

### Multi-factor Authentication

You can use options below to configure multi-factor authentication settings based on users/groups, device, and location data. Multi-factor authentication is required if there is a match for any of the specified requirements.

**Global Settings**

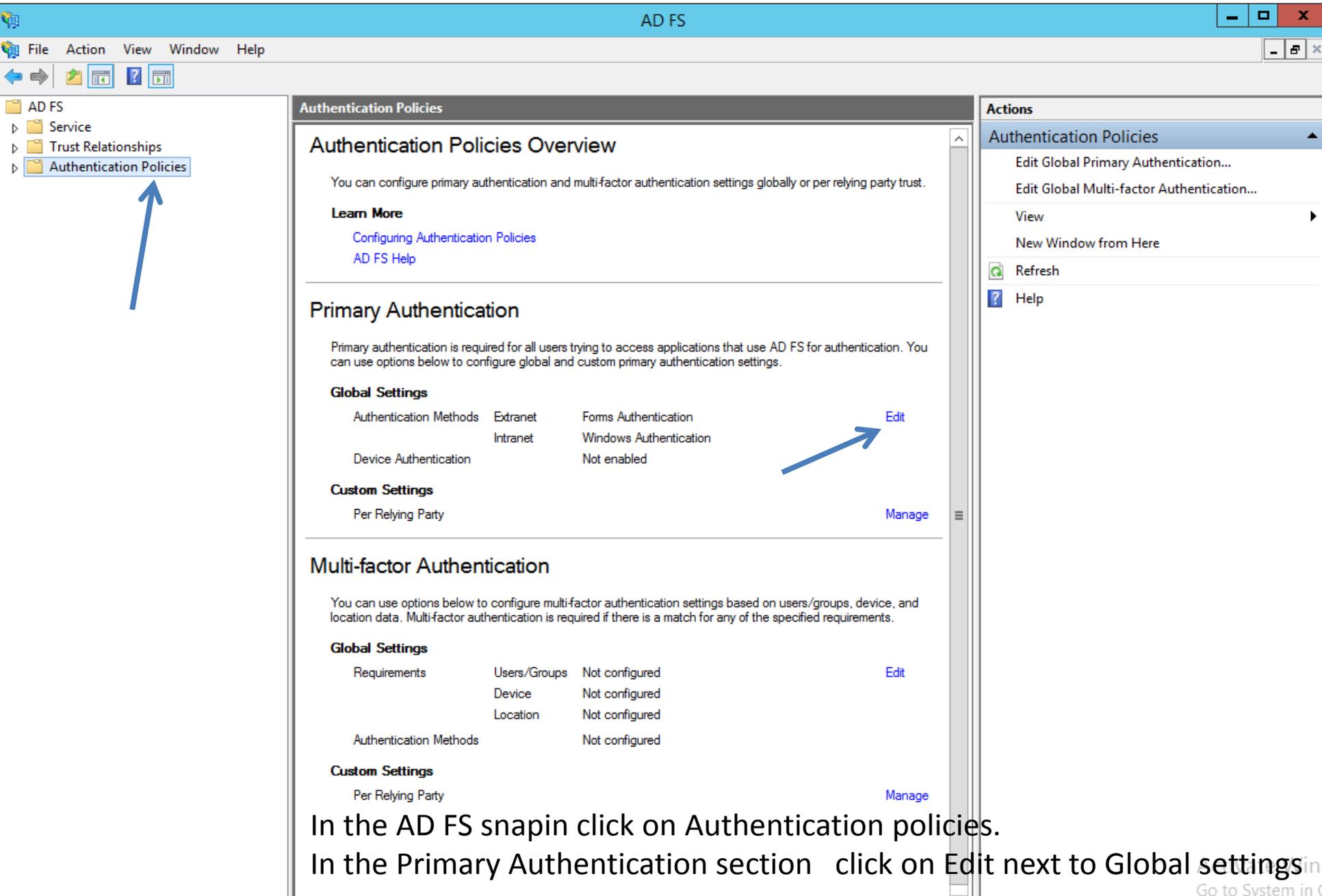
Requirements	Users/Groups	Not configured	<a href="#">Edit</a>
	Device	Not configured	
	Location	Not configured	
Authentication Methods		Not configured	

**Custom Settings**

Per Relying Party	<a href="#">Manage</a>
-------------------	------------------------

### Actions

- Authentication Policies
- Edit Global Primary Authentication...
- Edit Global Multi-factor Authentication...
- View
- New Window from Here
- Refresh
- Help



In the AD FS snapin click on Authentication policies.

In the Primary Authentication section click on Edit next to Global settings in

**Edit Global Authentication Policy**

Primary Multi-factor

Select authentication methods. By selecting more than one authentication method, you enable users to have a choice of what method to authenticate with at sign in.

If Integrated Windows authentication method is specified, it appears as the default authentication method on browsers that support Integrated Windows authentication.

Extranet

- Forms Authentication
- Certificate Authentication

Intranet

- Forms Authentication
- Windows Authentication
- Certificate Authentication

Enable device authentication

OK Cancel Apply

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**.

The screenshot shows the AD FS console interface. The left-hand navigation pane displays a tree view with 'AD FS' expanded to show 'Authentication Policies'. The main content area is titled 'Authentication Policies Overview' and contains three sections: 'Primary Authentication' and 'Multi-factor Authentication'. Each section has a table of settings with 'Edit' or 'Manage' links. A blue arrow points to the 'Edit' link for 'Global Settings' in the Multi-factor Authentication section. The right-hand 'Actions' pane is open, showing options like 'Edit Global Primary Authentication...' and 'Edit Global Multi-factor Authentication...'. The top of the window has a blue header with 'AD FS' and a menu bar with 'File', 'Action', 'View', 'Window', and 'Help'.

Setting	Value	Action
Authentication Methods	Extranet, Intranet	Edit
Device Authentication	Not enabled	

Setting	Value	Action
Requirements	Users/Groups, Device, Location	Edit
Authentication Methods	Not configured	

Edit Global Authentication Policy ✕

Primary **Multi-factor**

Configure multi-factor authentication (MFA) settings.

Users/Groups  
MFA is required for the following users and groups:

Devices  
MFA is required for the following devices:

Unregistered devices

Registered devices

Locations  
MFA is required when accessing applications from the following locations:

Extranet

Intranet

Select additional authentication methods. You must select at least one of the following methods to enable MFA:

Certificate Authentication

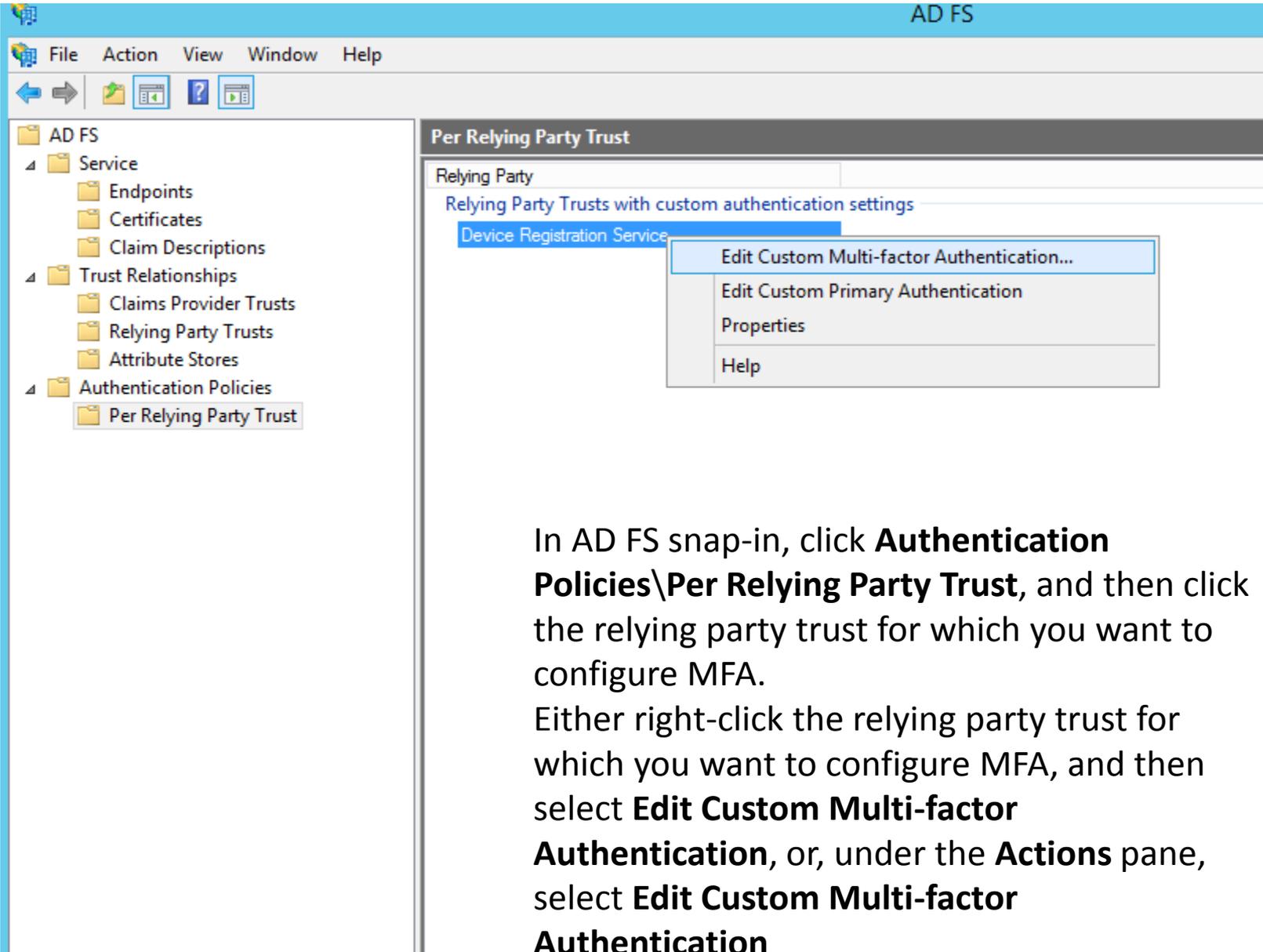
[What is multi-factor authentication?](#)

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



The screenshot shows the AD FS console interface. The left-hand navigation pane is expanded to show the following structure:

- AD FS
  - Service
    - Endpoints
    - Certificates
    - Claim Descriptions
  - Trust Relationships
    - Claims Provider Trusts
    - Relying Party Trusts
    - Attribute Stores
  - Authentication Policies
    - Per Relying Party Trust

The main pane displays the 'Per Relying Party Trust' configuration for a specific trust. The 'Relying Party' field is populated with 'Device Registration Service'. Below this, the text 'Relying Party Trusts with custom authentication settings' is visible. A context menu is open over the 'Device Registration Service' entry, with the following options:

- Edit Custom Multi-factor Authentication...
- Edit Custom Primary Authentication
- Properties
- Help

The 'Edit Custom Multi-factor Authentication...' option is highlighted in blue.

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**

Edit Authentication Policy for Device Registration Service ✕

Primary **Multi-factor**

Configure multi-factor authentication (MFA) settings.

**i** Global multi-factor authentication settings will apply to this relying party trust.

Users./Groups  
MFA is required for the following users and groups:

Devices  
MFA is required for the following devices:

Unregistered devices

Registered devices

Locations  
MFA is required when accessing applications from the following locations:

Extranet

Intranet

[What is 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.