



Integrations

ADFS Authentication

V5.1.0

CONTENTS

1 ADFS Authentication Application	1
2 Installing the Application	2
2.1 Prerequisite	2
2.2 Installing the ADFS Application in LogPoint	2
2.3 Verifying the Installation	2
3 Configuring the Application	4
3.1 Configuring the ADFS Authentication	4
3.2 Configuring Default Settings	8
3.3 Mapping Roles	10
4 Login with ADFS Authentication	12
5 Managing ADFS Users	18
6 Uninstalling the Application	21
6.1 Uninstalling the ADFS Authentication Application in LogPoint	21
7 Appendix	22
7.1 Installing the Duo Security in the ADFS Server	22
7.2 Selecting Duo Security in the ADFS Server	27

CHAPTER
ONE

ADFS AUTHENTICATION APPLICATION

The ADFS Authentication application enables you to log into LogPoint using *Microsoft's Active Directory Federation Services (ADFS)*. ADFS provides you with single sign-on access to systems and applications located across trusted organizational units.

INSTALLING THE APPLICATION

2.1 Prerequisite

LogPoint v6.7.0 or later

2.2 Installing the ADFS Application in LogPoint

1. Go to *Settings >> System >> Applications*.
2. Click **Import**.
3. **Browse** for the location of the downloaded pak file for ADFS application.
4. Click **Upload**.

2.3 Verifying the Installation

1. Go to the **LogPoint login** page.
2. Click the **Other Authentication Options** link. You can find the **AD FS Authentication** login option.

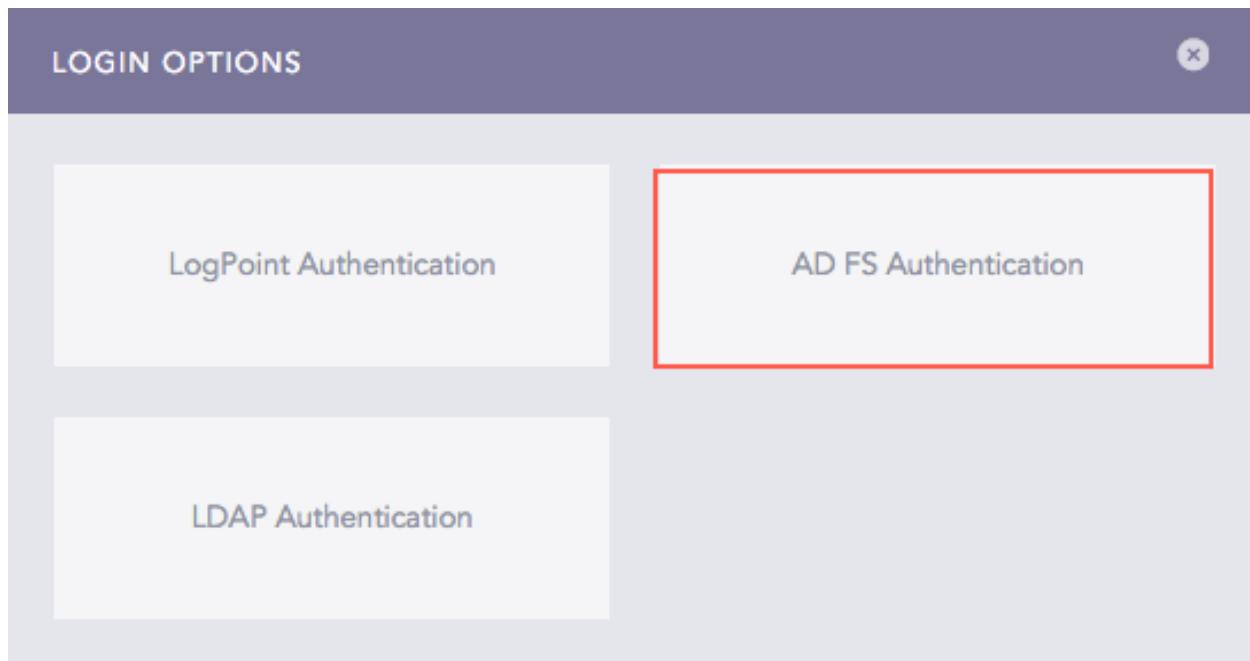


Fig. 1: AD FS Authentication Login Option

CONFIGURING THE APPLICATION

3.1 Configuring the ADFS Authentication

1. Go to *Settings* >> *System* >> *Plugins*.
2. Find **AD FS Authentication v5.1.0** and click **Manage**.

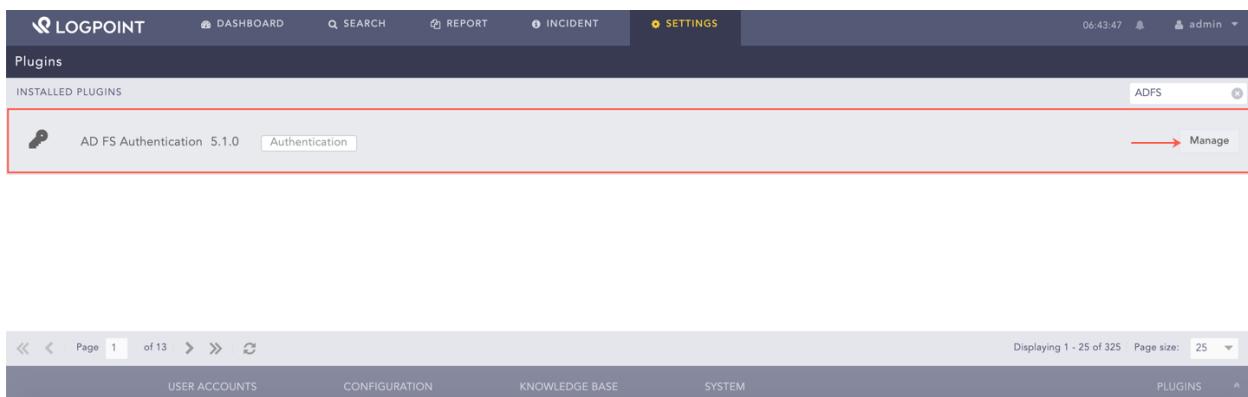


Fig. 1: Manage AD FS Authentication

3. Click **Add Server**.



Fig. 2: Add ADFS Server

4. Enter a unique **Server Name**.

Note: For details on ADFS server side configuration, refer to the [Microsoft's documentation for Active Directory Federation Services](#).

5. Enter the fully qualified domain name of your ADFS server in the **AD FS URL** text box. LogPoint users will be redirected to this domain for authentication.

6. Copy the automatically generated **AD FS Endpoint URL**, which you will need while configuring LogPoint in your ADFS server. While adding LogPoint as a Relying Party Trust in the ADFS server, on the **Configure URL** page, select the **Enable support for the SAML 2.0 Web SSO protocol** option and provide the **AD FS Endpoint URL** in the **Relying party SAML 2.0 SSO service URL** text box.
7. Enter the *Relying party identifier* in the **Issuer** text box. You can find the *Relying party identifier* under the **Identifier** column of the **Relying Party Trust** panel of your ADFS server.
8. Provide the token-signing certificate of your ADFS server in the **AD FS Certificate** text box. You can obtain the certificate from the **Certificates** panel of the ADFS server. Export the certificate in the *Base-64 encoded X.509 (.CER)* format, and copy the content in the **AD FS Certificate** text box.
9. Enter the **Response Username Field** and **Response Role Field**, which are used to extract the username and role from the ADFS server.

After adding LogPoint as a Relying Party Trust in the ADFS server, you need to create claim rules for username and role. While creating the claim rules, you must map the LDAP attributes to two outgoing claim types. One of the claim type needs to be *Role* for the role, and another can be any other attribute for the username. After creating the rules, go to the **Edit Claim Rules** page and select the created rule. Then, click **View Rule Language**. The **Response Username Field** and **Response Role Field** are the values of the **types** parameter.

10. Click **Save**.

X

AD FS SERVER INFORMATION

AD FS SERVER

Server Name

AD FS URL

AD FS Endpoint URL

ISSUER

AD FS CERTIFICATE

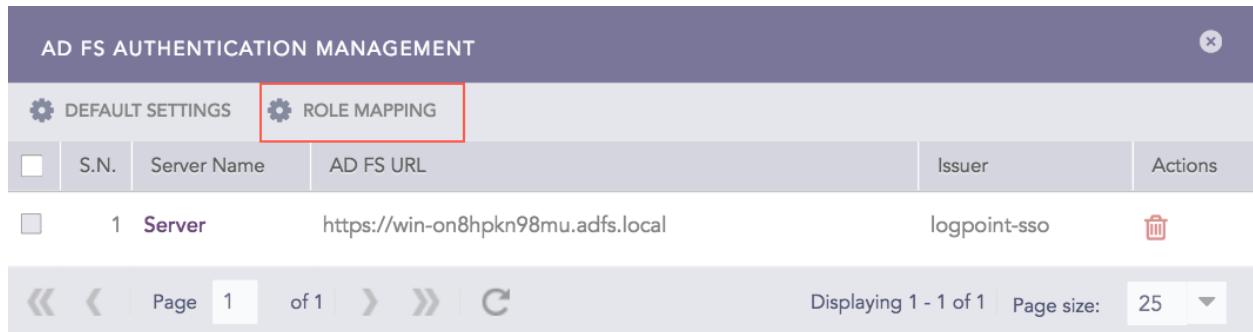
```
-----BEGIN CERTIFICATE-----
MIIC8DCCAdigAwIBAgIQIAI9gvwTn6RLrZOBe3srpTANBgkqhkiG9w0BAQsFADA0
MTIwMAYDVQQDEyIBREZTIFNpZ25pbmcgLSBXSU4tT044SFBLTjk4TVUuYWRmcy5s
b2NhbDAeFw0xODA2MDcwNzE3MjhaFw0xOTA2MDcwNzE3MjhaMDQxMjAwBgNVBAMT
KUFERIMgU2lnbmluZyAtIFdTjI1PTjhIUEtOOThNVS5hZGZzLmxvY2FsMIIIBljAN
BgkqhkiG9w0BAQEFAAOCAQ8AMIIIBCgKCAQEAzBSuOXvWB2QQCZ4lbvZhF7agac0B
oiWDTBt0z1rlB42bncSkW6wCNm0dwzKl6bUdzMDdZAewL4D0prT/7sTRj32PCvB2
iFMcO+dfDfJ5r565vnwBtByWJVJHRIXQSpNXGzxdpmLs77m7pCaI5VBFdtWNb4Zx
4Q9ip+2+BbSmVMZly3J2mWfNO/LKEtIJ+xhAJftL9DRamkSKig+nIxpyPKTuFLrJ
J+wnyaj5sCBZhL0+t9F88PaVNQlaPlm/YGT94UVBUDBOHRPcPe1dExvqrGb+W1dc
iddTHYv2k5awJa3fEtxIQDRPaVPva7OV5D6nIeaOuUYPZXhXvVN1WvaYAwIDAQAB
-----END CERTIFICATE-----
```

Response Username Field

Save
Cancel

Fig. 3: AD FS Server Information Panel

Note: Once you configure the ADFS Authentication application, the panel removes the **Add Server** option and includes the **Roles Mapping** option.



S.N.	Server Name	AD FS URL	Issuer	Actions
1	Server	https://win-on8hpkn98mu.adfs.local	logpoint-sso	

Fig. 4: Add ADFS Server

3.2 Configuring Default Settings

1. Click the **Default Settings**.
2. Select a LogPoint user group as the **Default Role**. The application assigns the user group to the ADFS users whose role attribute has not been returned by the ADFS server.
3. Click **Save**.

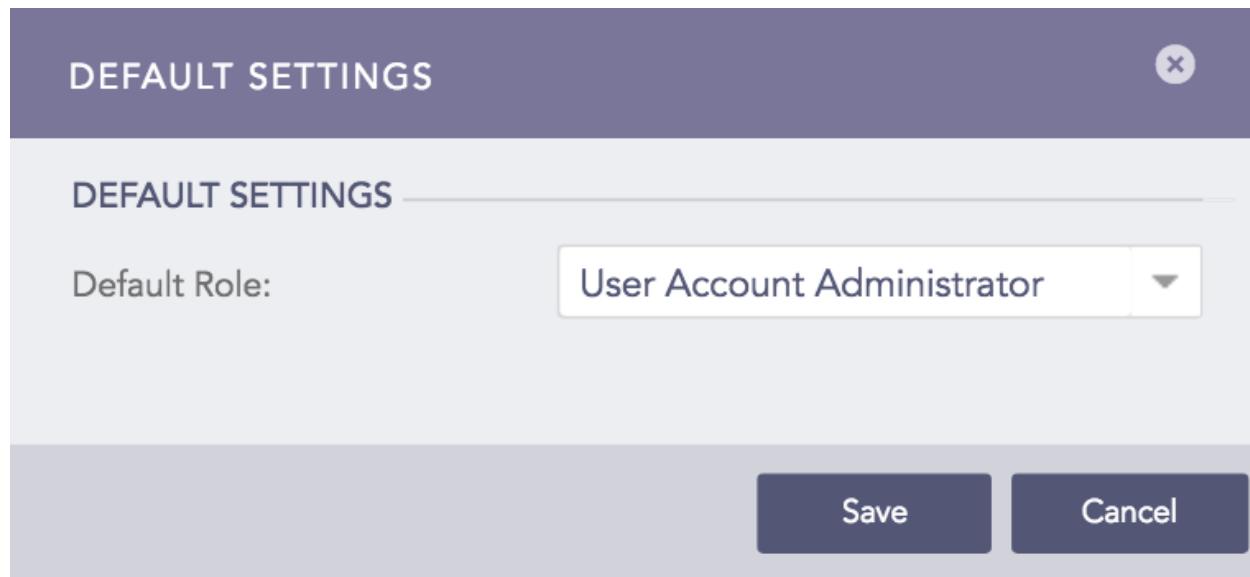


Fig. 5: Default Settings Panel

3.3 Mapping Roles

You can map an ADFS role to a LogPoint user group to define access permission on LogPoint.

Follow these steps to map an ADFS role to a LogPoint user group:

1. Click **Roles Mapping**.

S.N.	Server Name	AD FS URL	Issuer	Actions
1	Server	https://win-on8hpkn98mu.adfs.local	logpoint-sso	

Fig. 6: Adding Role Mapping

2. Enter an **AD FS Role**.
3. Select a **LogPoint User Group** to assign to the AD FS role mentioned above.
4. Click **Add**. A table lists all the mapped ADFS roles and LogPoint user groups. You can either edit or delete the added role mappings from the table.

S.N.	AD FS Role	LogPoint User Group	Actions
1	Admin	LogPoint Administrator	

Fig. 7: ADFS Role Mapping

ROLE MAP STRATEGIES

MAPPING INFORMATION

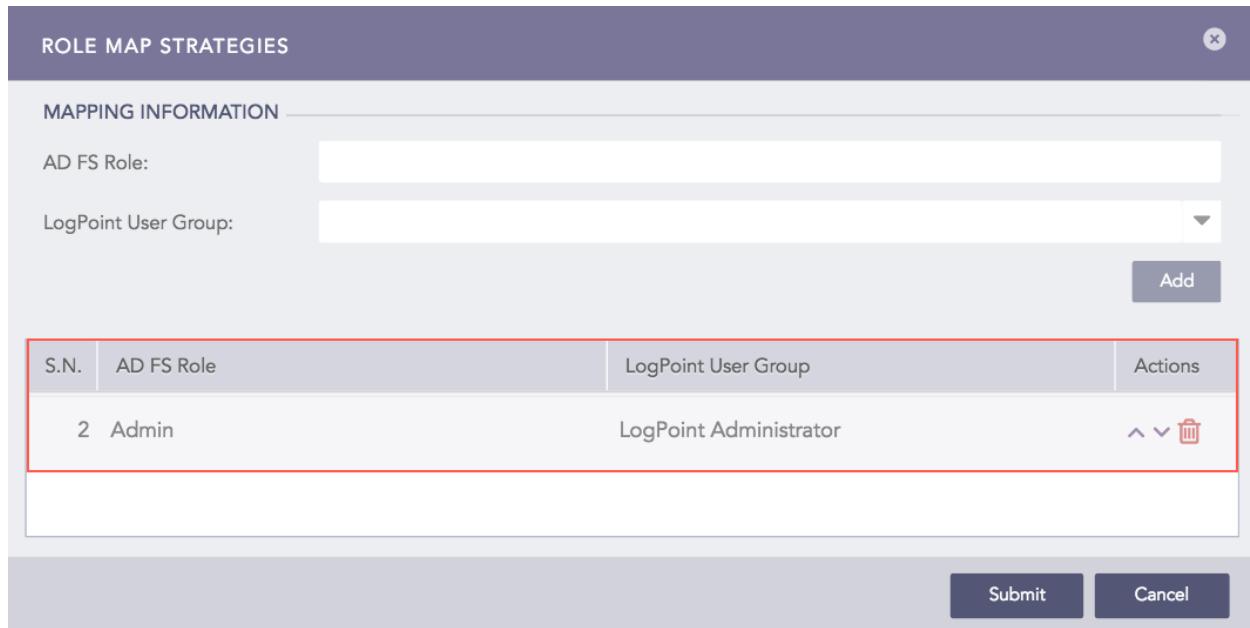
AD FS Role:

LogPoint User Group: ▼

Add

S.N.	AD FS Role	LogPoint User Group	Actions
2	Admin	LogPoint Administrator	^ ▼ trash

Submit **Cancel**



The screenshot shows the 'ROLE MAP STRATEGIES' section of the ADFS Authentication application. Under 'MAPPING INFORMATION', there are fields for 'AD FS Role' and 'LogPoint User Group', both currently empty. A large 'Add' button is visible. Below this is a table with a single row. The table has columns for 'S.N.', 'AD FS Role', 'LogPoint User Group', and 'Actions'. The 'Actions' column contains icons for moving up (^), moving down (▼), and deleting (trash). The table row shows '2 Admin' mapped to 'LogPoint Administrator'. At the bottom are 'Submit' and 'Cancel' buttons.

Fig. 8: ADFS Role Mapping Added

Note:

- Mapping roles in the ADFS Authentication application is mandatory.
- The ADFS role to LogPoint user group mapping is one-to-one, which means you can map an ADFS role to a single LogPoint user group only.

CHAPTER
FOUR

LOGIN WITH ADFS AUTHENTICATION

After configuring the ADFS Authentication, you can log into LogPoint using the ADFS credentials.

Follow these steps to log in with the ADFS Authentication:

1. Go to the **LogPoint login** page.
2. Click the **Other Authentication Options** link.

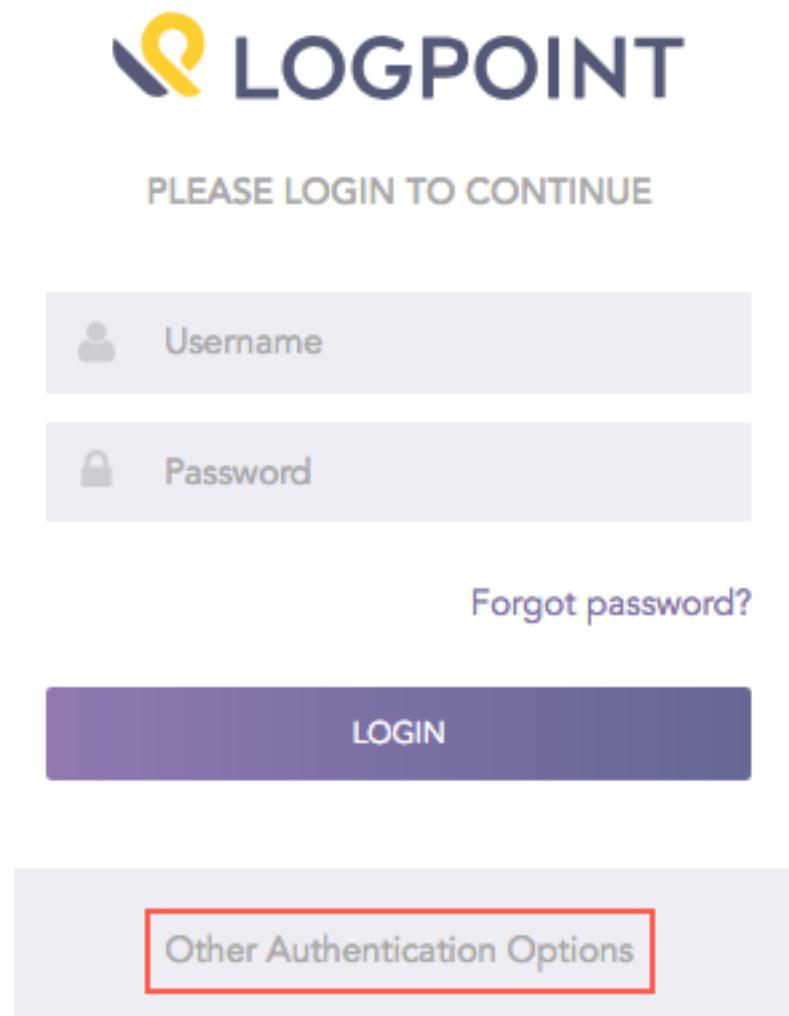


Fig. 1: Other Authentication Options

3. Select **AD FS Authentication**.

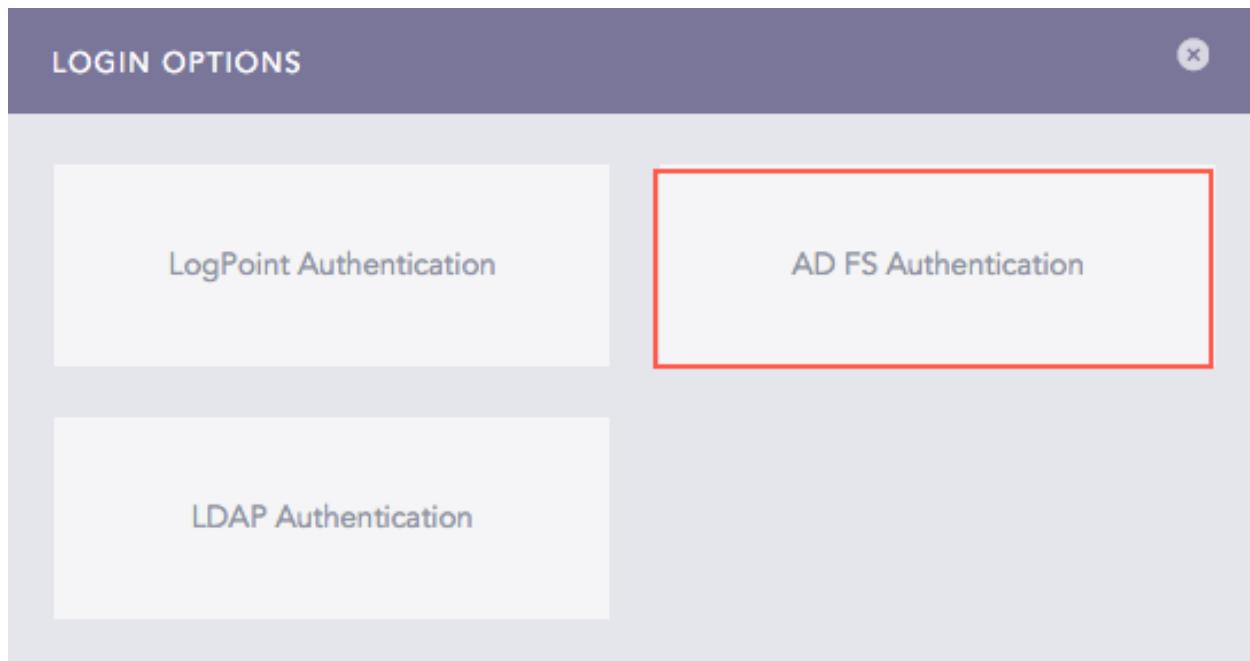


Fig. 2: Login Options

4. Click **Login**.

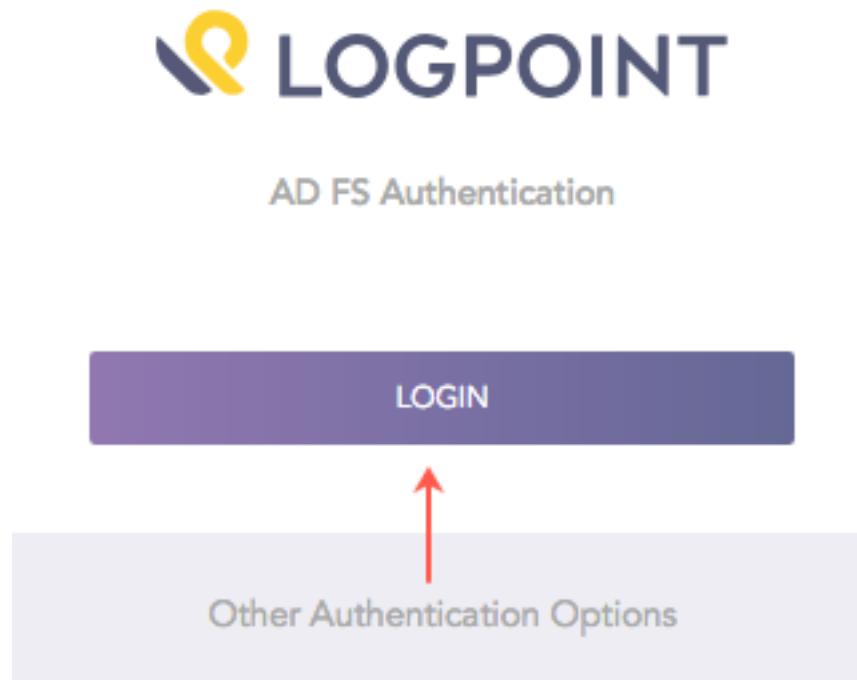


Fig. 3: ADFS Authentication Login

5. Enter your ADFS **Username** and **Password**.
6. Click **Sign in** to log into LogPoint.

Account ADFS

Sign in with your organizational account

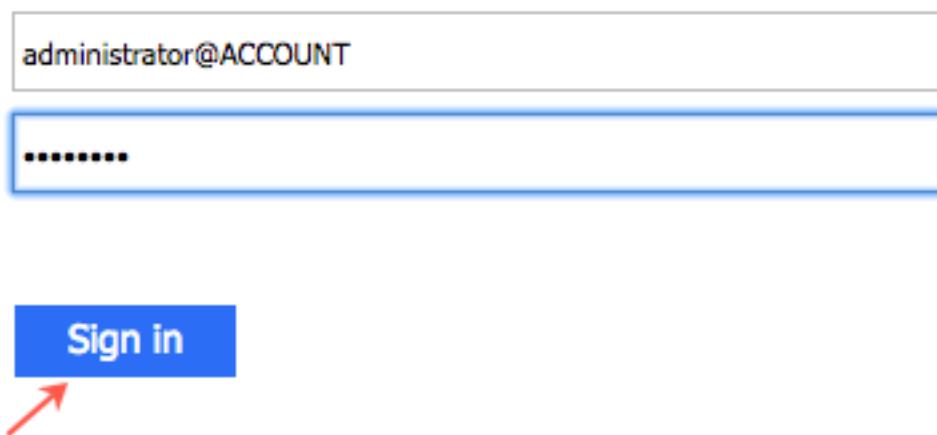


Fig. 4: ADFS Server Login

Important:

- The time zones of the ADFS server and LogPoint must be identical.
- If you have configured the Duo Security in your ADFS server, you need to further verify with the Duo's two-factor authentication. For more details, refer to the [Duo Security Manual](#).
- Refer to the [Appendix](#) section to obtain information on installing and configuring the Duo Security in the ADFS server.

Once you log in with the ADFS credentials, the system adds `adfs` as a prefix to your username. For example, if you log in as `bob` with the AD FS Authentication option, LogPoint updates your username as `adfs_bob`.

The screenshot shows the LogPoint application interface. At the top, the navigation bar includes 'LOGPOINT', 'DASHBOARD', 'SEARCH', 'REPORT', 'INCIDENT', 'SETTINGS', the time '08:45:47', and a user dropdown set to 'adfs_bob'. The main content area is divided into several sections:

- System Settings**: Configure LogPoint Name, IP Address, DNS, SMTP, and SNMP.
- Applications**: Import applications containing knowledge base information. Options include Normalization Package, Search Package, Report Package, Dashboard Package, Label Package, and Plugins.
- Repos**: Create repositories with defined retention policies where logs are stored. It's noted that more than one place can be used to store logs.
- Devices and Device Groups**: Configure Log Parsers, Collectors, Fetchers, and Device Groups. Categories include Parsers, Device Groups, and Devices.
- Users and Groups**: Create users and groups. Options include Setup permissions based on permission groups, Assign permission groups to user groups, and Add users to the user groups.
- My Preferences**: Configure settings like Time zone, Change your password, Notification, Log fetching, Date time display format, and Log fields to be shown on the search results.
- Search**: Search for logs or tables in the system. It's noted that search results can be viewed in tabular form or as graphical charts and timecharts.
- Dashboards**: Import dashboards from dashboard packages. You can create your own dashboards by clicking the '+' tab next to the Quick Start tab.
- Reports**: Use reports templates to schedule and create ad-hoc reports in formats like PDF, XLS, HTML, DocX, and XML.

Fig. 5: User Logged In with ADFS Authentication

Note: Once you log in with the ADFS Authentication, you get signed into LogPoint for a period of session time. You can define the session time in the ADFS server.

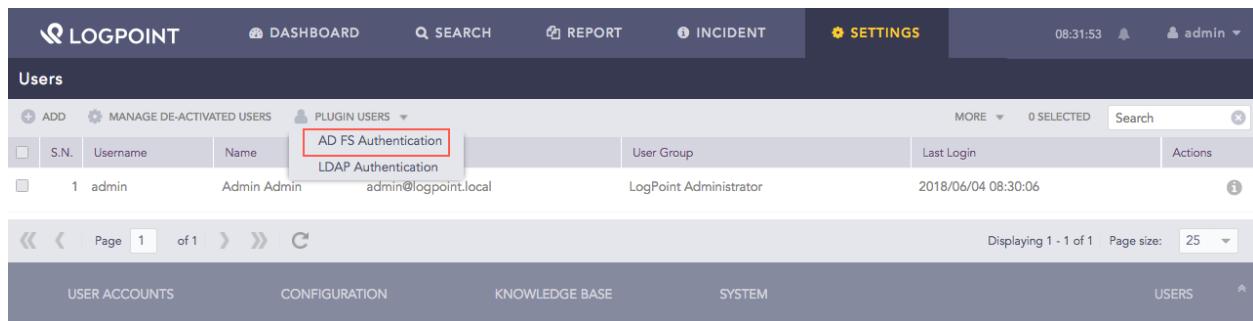
CHAPTER FIVE

MANAGING ADFS USERS

LogPoint users with sufficient privileges can manage ADFS users.

Follow these steps to manage ADFS users:

1. Go to *Settings* >> *System* >> *User Accounts*.
2. Click **Users**.
3. In the **Plugin Users** drop-down menu, click **AD FS Authentication**.

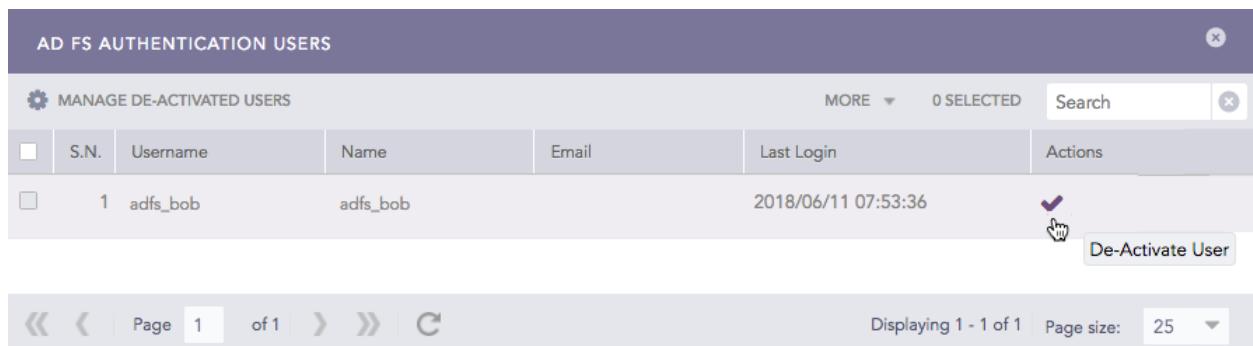


The screenshot shows the LogPoint web interface with the following details:

- Header:** LOGPOINT, DASHBOARD, SEARCH, REPORT, INCIDENT, SETTINGS, 08:31:53, admin.
- Section:** Users
- Sub-section:** AD FS Authentication (highlighted with a red box)
- Table:** A list of users under AD FS Authentication. The columns are: S.N., Username, Name, User Group, Last Login, and Actions.
- Data:** One user listed: S.N. 1, Username: admin, Name: Admin Admin, User Group: LogPoint Administrator, Last Login: 2018/06/04 08:30:06, Actions: De-Activate User (highlighted with a red box).
- Page Navigation:** Page 1 of 1, displaying 1-1 of 1, page size 25.
- Footer:** USER ACCOUNTS, CONFIGURATION, KNOWLEDGE BASE, SYSTEM, USERS.

Fig. 1: Plugin Users

4. Click the **De-Activate User** icon in the **Actions** column to deactivate a user.



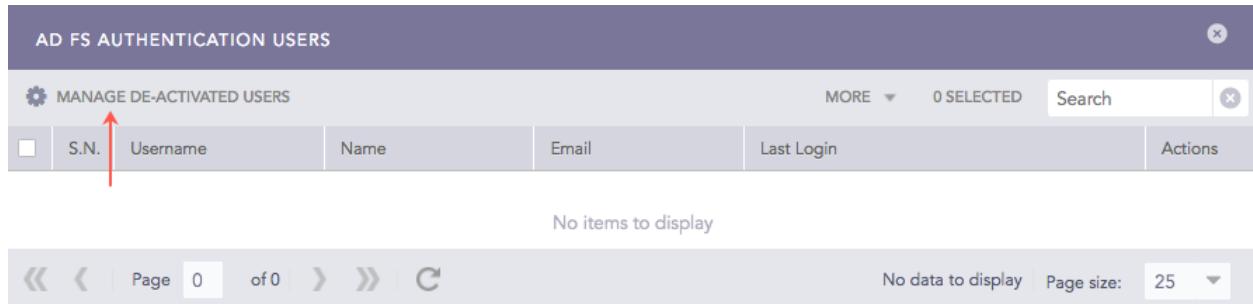
The screenshot shows the 'AD FS AUTHENTICATION USERS' list with the following details:

- Section:** AD FS AUTHENTICATION USERS
- Sub-section:** MANAGE DE-ACTIVATED USERS
- Table:** A list of users under AD FS AUTHENTICATION USERS. The columns are: S.N., Username, Name, Email, Last Login, and Actions.
- Data:** One user listed: S.N. 1, Username: adfs_bob, Name: adfs_bob, Last Login: 2018/06/11 07:53:36, Actions: De-Activate User (highlighted with a red box).
- Page Navigation:** Page 1 of 1, displaying 1-1 of 1, page size 25.

Fig. 2: De-Activate ADFS Users

5. Click **Yes**.

6. Click **Manage De-Activated Users**.



AD FS AUTHENTICATION USERS

MANAGE DE-ACTIVATED USERS

S.N. Username Name Email Last Login Actions

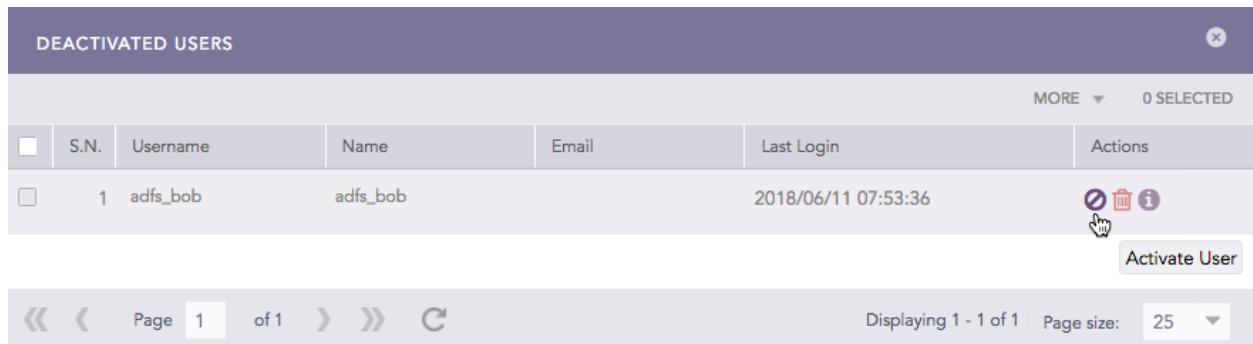
No items to display

Page 0 of 0

No data to display Page size: 25

Fig. 3: Manage De-Activated ADFS Users

7. Click the **Activate User** icon to activate or the **Delete** icon to delete the deactivated user.



DEACTIVATED USERS

S.N. Username Name Email Last Login Actions

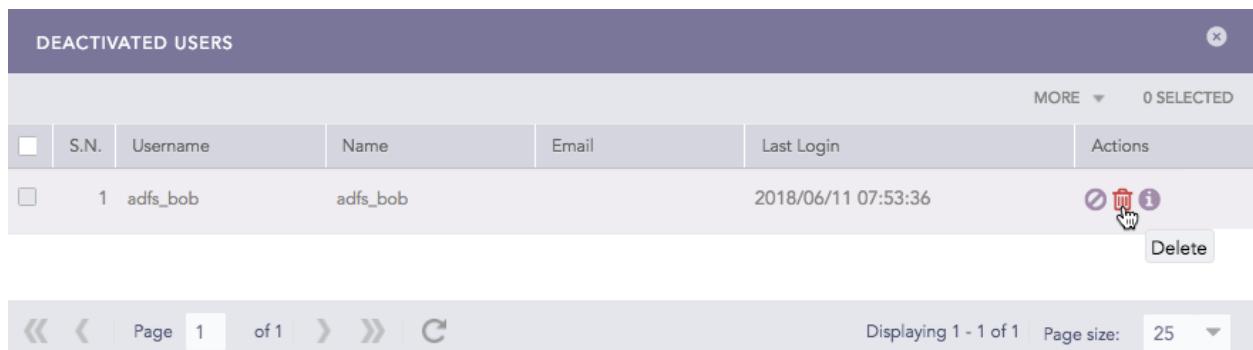
1 adfs_bob adfs_bob 2018/06/11 07:53:36

Activate User

Page 1 of 1

Displaying 1 - 1 of 1 Page size: 25

Fig. 4: Activate the De-Activated ADFS User



DEACTIVATED USERS

S.N. Username Name Email Last Login Actions

1 adfs_bob adfs_bob 2018/06/11 07:53:36

Delete

Page 1 of 1

Displaying 1 - 1 of 1 Page size: 25

Fig. 5: Delete the De-Activated ADFS User

UNINSTALLING THE APPLICATION

6.1 Uninstalling the ADFS Authentication Application in LogPoint

1. Go to *Settings* >> *System* >> *Applications*.
2. Click the **Uninstall** (trash) icon from the **Actions** column.

Note: You must remove the **ADFS Authentication** configuration to delete the application.

CHAPTER
SEVEN

APPENDIX

The following section guides you through the process of installing and configuring the Duo Security in the ADFS server.

7.1 Installing the Duo Security in the ADFS Server

1. Launch the Duo AD FS installer package provided by *Duo Security* in the ADFS server.
2. Click **Next**.



Fig. 1: Duo AD FS MFA Adapter Setup

3. Enter the **Integration key**.
4. Enter the **Secret key**.
5. Enter the **API hostname**.

Note: Refer to the **Appendix** section of the **Duo Security Manual** to retrieve the **Integration key**, the **Secret key**, and the **API hostname**.

6. Select **Bypass Duo authentication when offline** to enable login when the **Duo Security** is offline.

7. Click **Next**.

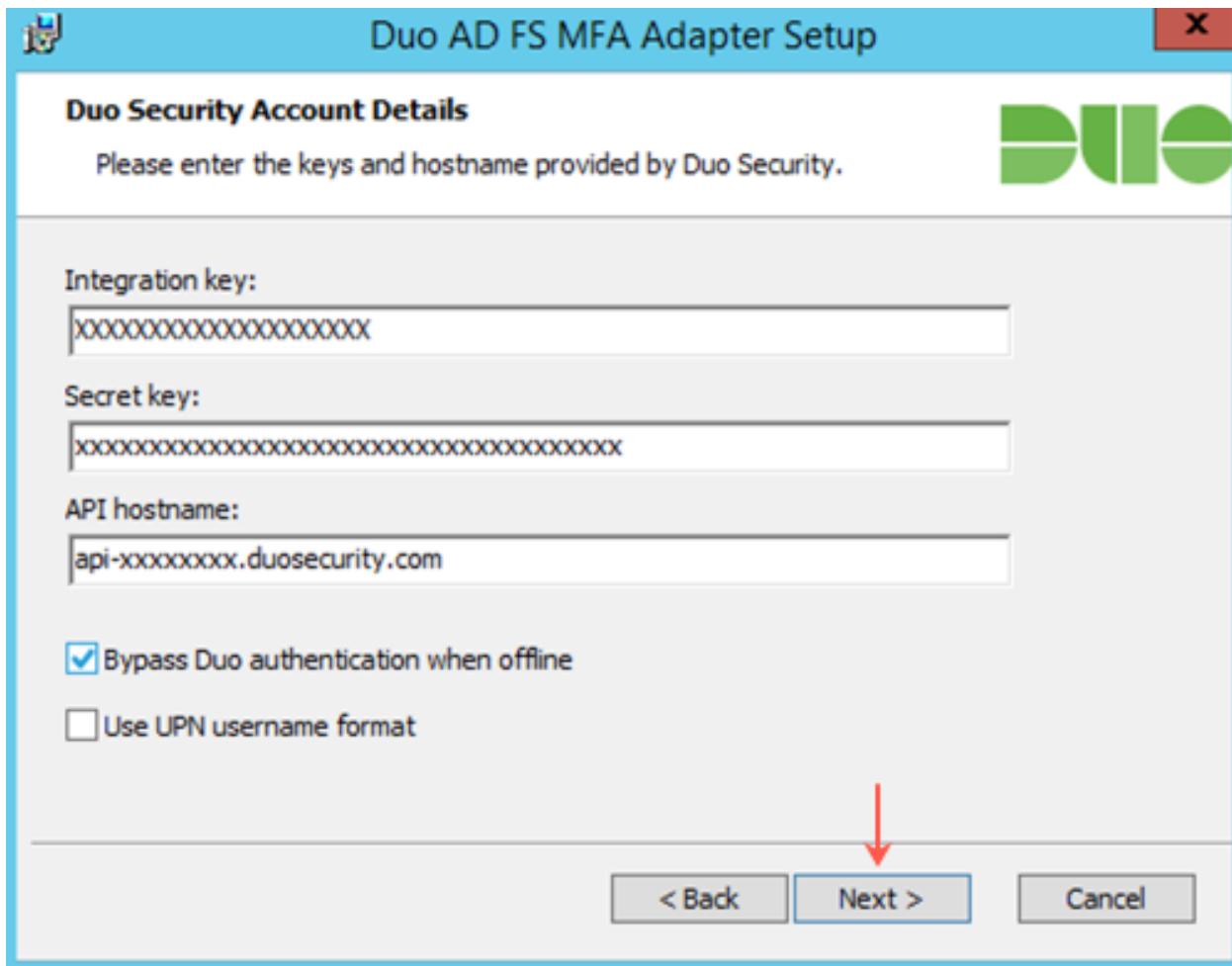


Fig. 2: Duo Security Account Details

8. Select **Generate new session key**.

9. Click **Next**.

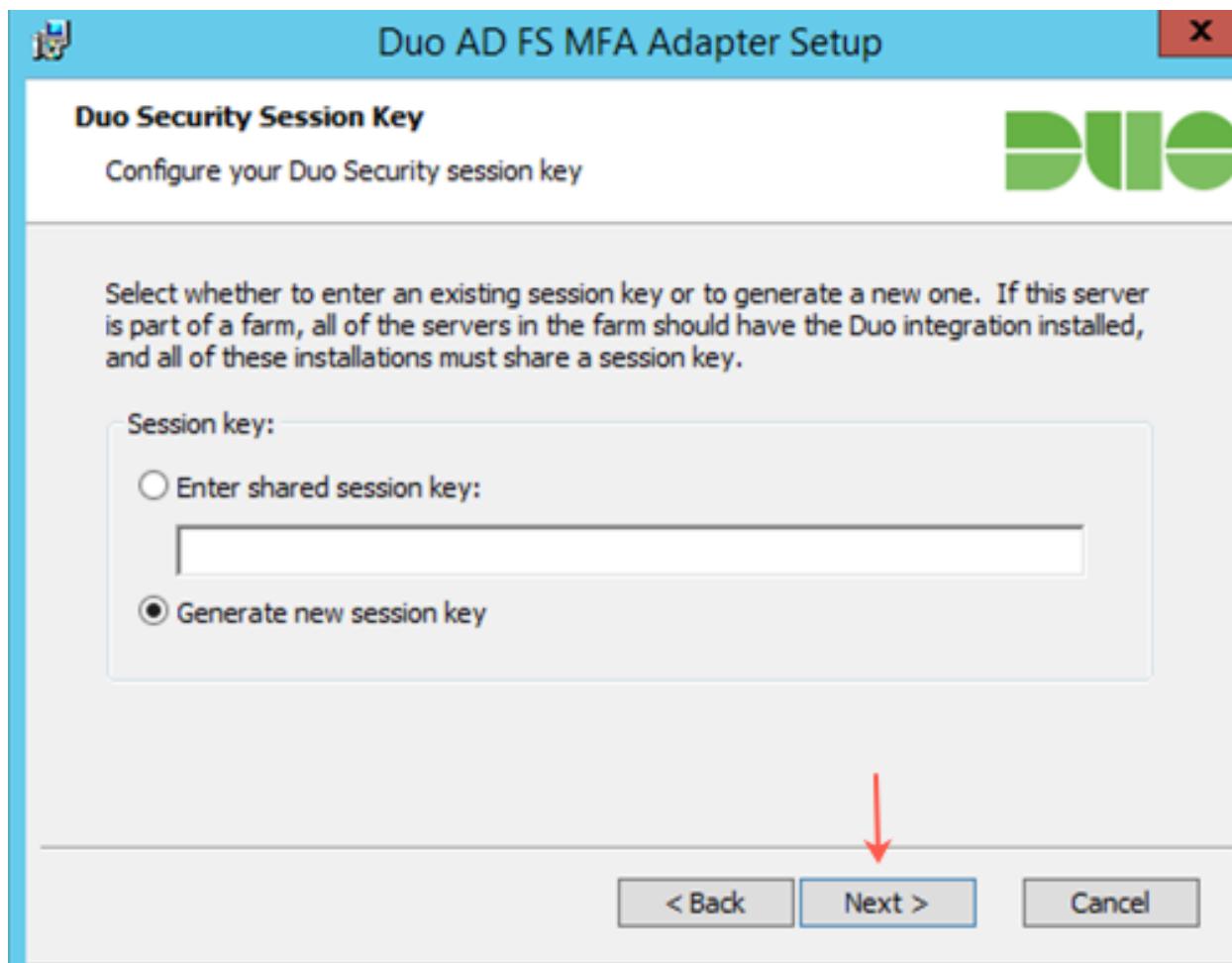


Fig. 3: Generating New Duo Security Session Key

10. Click **Install**.

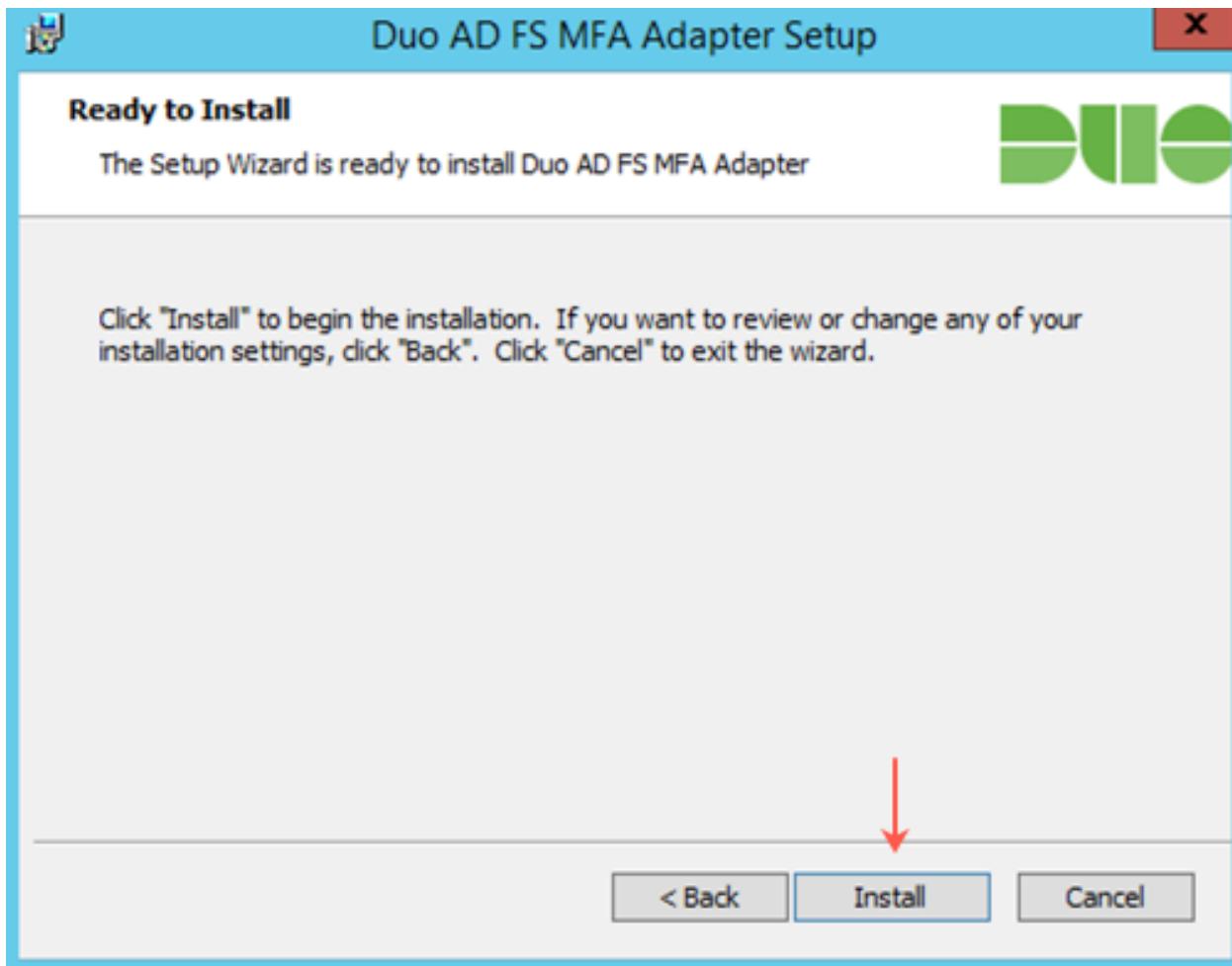


Fig. 4: Installing Duo AD FS MFA Adapter

11. Click **Finish**.



Fig. 5: Completing the Duo AD FS MFA Adapter Setup Wizard

7.2 Selecting Duo Security in the ADFS Server

1. Go to the AD FS Server >> AD FS >> Authentication Policies.

2. Click **Edit Global Multi-factor Authentication**.

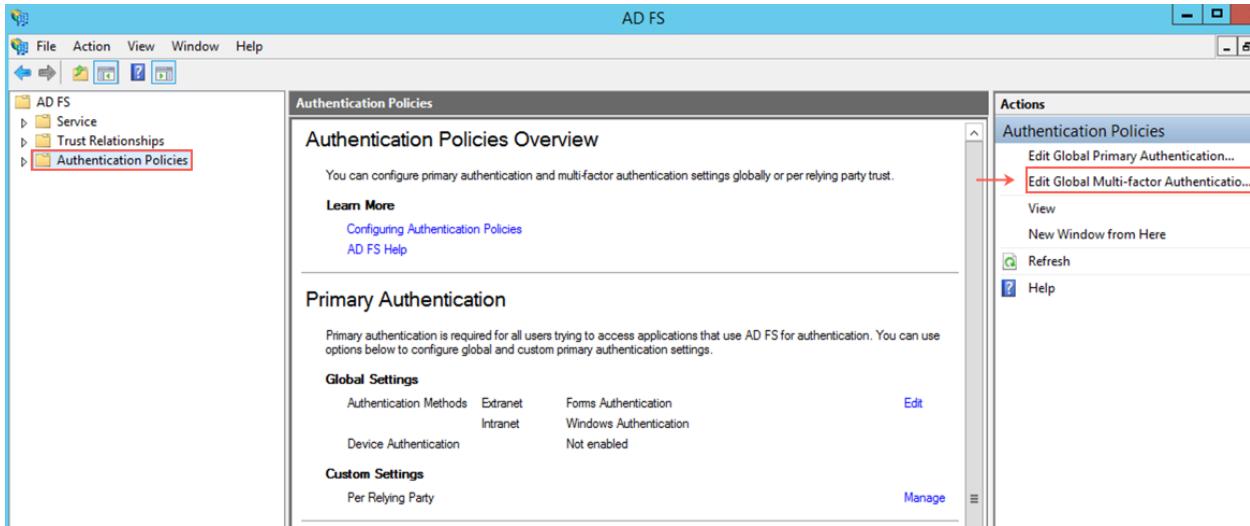


Fig. 6: Authentication Policies

3. Select **Duo Authentication** for AD FS 1.2.0.17.

4. Click **OK**.

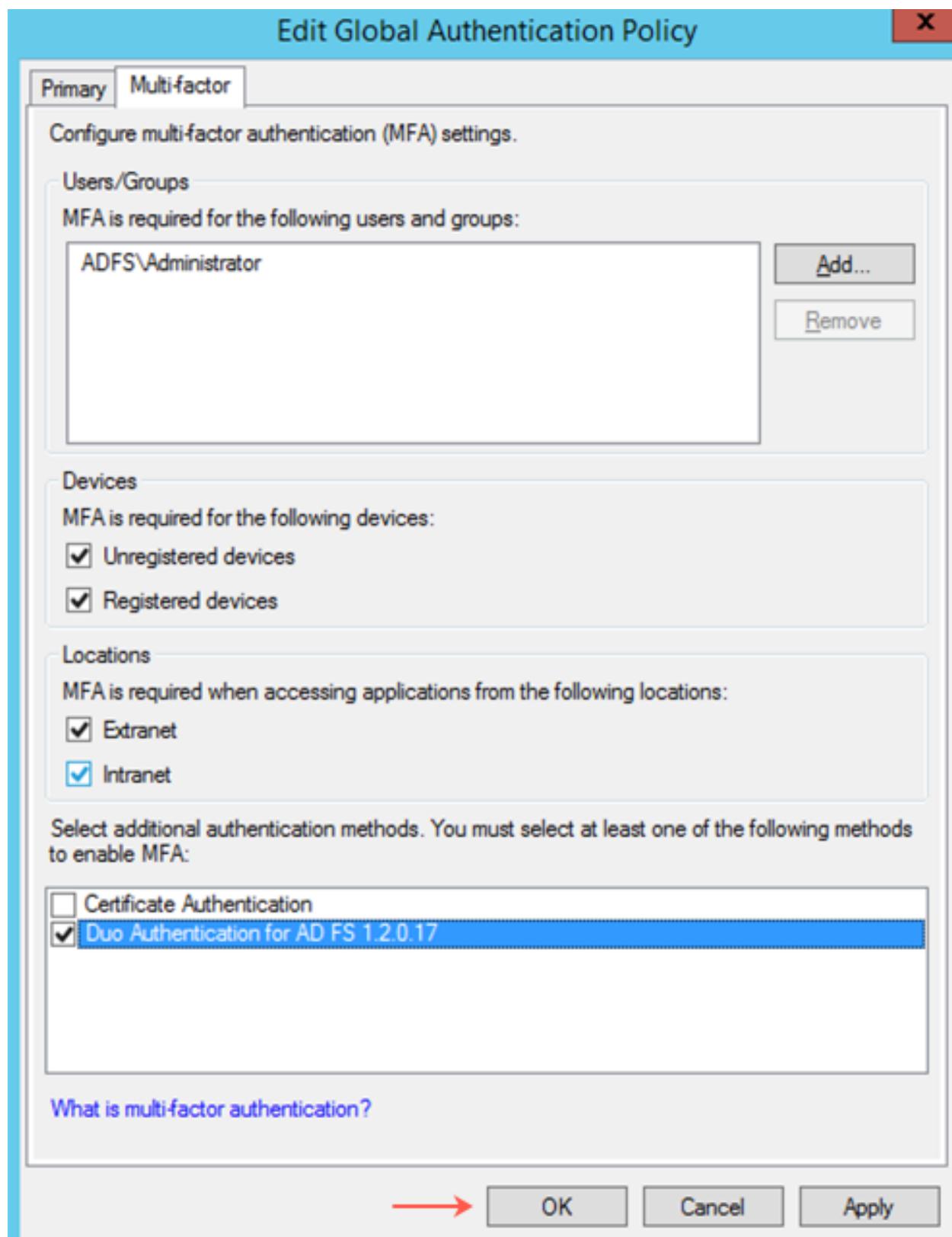


Fig. 7: Edit Global Authentication Policy Panel