



# **Configuring OnCommand Workflow Automation**

**OnCommand Workflow Automation 5.1**

NetApp  
August 30, 2024

# Table of Contents

- Configuring OnCommand Workflow Automation ..... 1
  - Configure AutoSupport ..... 1
  - Configure authentication settings ..... 2
  - Add Active Directory groups ..... 3
  - Configure email notifications ..... 3
  - Configure SNMP ..... 3
  - Configure Syslog ..... 4
  - Configure protocols for connecting to remote systems ..... 4

# Configuring OnCommand Workflow Automation

OnCommand Workflow Automation (WFA) enables you to configure various settings—for example, AutoSupport and notifications.

When configuring WFA, you can set up one or more of the following, as required:

- AutoSupport for sending AutoSupport messages to technical support
- Microsoft Active Directory Lightweight Directory Access Protocol (LDAP) server for LDAP authentication and authorization for WFA users
- Mail for email notifications about workflow operations and sending AutoSupport messages
- Simple Network Management Protocol (SNMP) for notifications about workflow operations
- Syslog for remote data logging

## Configure AutoSupport

You can configure several AutoSupport settings such as the schedule, content of the AutoSupport messages, and the proxy server. AutoSupport sends weekly logs of the content that you selected to technical support for archiving and issue analysis.

### Steps

1. Log in to WFA through a web browser as an admin.
2. Click **Settings**, and under **Setup** click **AutoSupport**.
3. Ensure that the **Enable AutoSupport** box is selected.
4. Enter the required information.
5. Select one of the following from the **Content** list:

If you want to include...	Then choose this option...
Only configuration details such as users, workflows, and commands of your WFA installation	send only configuration data
WFA configuration details and data in WFA cache tables such as the scheme	send configuration and cache data (default)
WFA configuration details, data in WFA cache tables, and data in the installation directory	send configuration and cache extended data



The password of any WFA user is *not* included in the AutoSupport data.

6. Test that you can download an AutoSupport message:
  - a. Click **Download**.
  - b. In the dialog box that opens, select the location to save the `.7z` file.
7. Test the sending of an AutoSupport message to the specified destination by clicking **Send Now**.

8. Click **Save**.

## Configure authentication settings

You can configure OnCommand Workflow Automation (WFA) to use a Microsoft Active Directory (AD) Lightweight Directory Access Protocol (LDAP) server for authentication and authorization.

You must have configured a Microsoft AD LDAP server in your environment.

Only Microsoft AD LDAP authentication is supported for WFA. You cannot use any other LDAP authentication methods, including Microsoft AD Lightweight Directory Services (AD LDS) or Microsoft Global Catalog.



During communication, LDAP sends the user name and password in plain text. However, LDAPS (LDAP secure) communication is encrypted and secure.

### Steps

1. Log in to WFA through a web browser as an admin.
2. Add a list of Active Directory group names to the required roles.



You can add a list of AD group names to the required roles in the Active Directory Groups Window.

[Active Directory Groups window](#)

3. Click **Administration > WFA Configuration**.
4. In the WFA Configuration dialog box, click the **Authentication** tab, and then select the **Enable Active Directory** check box.
5. Enter the required information in the fields:
  - a. If you want to use the user@domain format for domain users, replace sAMAccountName with userPrincipalName in the **User name attribute** field.
  - b. If unique values are required for your environment, edit the required fields.

6. Click **Add** to add the Active Directory in the Active Directory Servers table with a URI format:

```
ldap://active_directory_server_address\[[:port]\]
```

```
ldap://NB-T01.example.com[:389]
```

If you have enabled LDAP over SSL, you can use the following URI format:

```
ldaps://active_directory_server_address\[[:port]\]
```

7. Provide the credentials to bind the LDAP server and the base DN.
8. Test the authentication of the given user:
  - a. Enter the user name and password.
  - b. Click **Test Authentication**.



You must have added the Active Directory Group to test the authentication of the given user in WFA.

9. Click **Save**.

## Add Active Directory groups

You can add Active Directory groups in OnCommand Workflow Automation (WFA).

### Steps

1. Log in to WFA through a web browser as an admin.
2. Click **Settings** and under **Management**, click **Active Directory Groups**.
3. In the Active Directory Groups window, click the **New** icon.
4. In the New Active Directory Group dialog box, enter the required information.

If you select **Approver** from the **Role** drop down list, it is recommended provide the email ID of the approver. If there are multiple approvers, you can provide a group email ID in the **E-mail** field. Select the different events of the workflow for which the notification is to be sent to the particular Active Directory group.

5. Click **Save**.

## Configure email notifications

You can configure OnCommand Workflow Automation (WFA) to send you email notifications about workflow operations—for example, workflow started or workflow failed.

You must have configured a mail host in your environment.

### Steps

1. Log in to WFA through a web browser as an admin.
2. Click **Settings**, and under **Setup** click **Mail**.
3. Enter the required information in the fields.
4. Test the mail settings by performing the following steps:
  - a. Click **Send test mail**.
  - b. In the Test Connection dialog box, enter the email address to which you want to send the email.
  - c. Click **Test**.
5. Click **Save**.

## Configure SNMP

You can configure OnCommand Workflow Automation (WFA) to send Simple Network Management Protocol (SNMP) traps about the status of workflow operations.

WFA now supports SNMP v1 and SNMP v3 protocols. SNMP v3 provides additional security features.

The WFA .mib file provides information about the traps that are sent by the WFA server. The .mib file is located in the <WFA\_install\_location>\wfa\bin\wfa.mib directory on the WFA server.



The WFA server sends all the trap notifications with a generic object identifier (1.3.6.1.4.1.789.1.1.12.0).

You cannot use SNMP community strings such as `community_string@SNMP_host` for SNMP configuration.

## Configure Syslog

You can configure OnCommand Workflow Automation (WFA) to send log data to a specific Syslog server for purposes such as event logging and log information analysis.

You must have configured the Syslog server to accept data from the WFA server.

### Steps



1. Log in to WFA through a web browser as an admin.
2. Click **Settings**, and under **Maintenance** click **Syslog**.
3. Select the **Enable Syslog** check box.
4. Enter the Syslog host name and select the Syslog log level.
5. Click **Save**.

## Configure protocols for connecting to remote systems

You can configure the protocol used by OnCommand Workflow Automation (WFA) to connect to remote systems. You can configure the protocol based on your organization's security requirements and the protocol supported by the remote system.

### Steps

1. Log in to WFA through a web browser as an admin.
2. Click **Data Source Design > Remote System Types**.
3. Perform one of the following actions:

If you want to...	Do this...
Configure a protocol for a new remote system	<ol style="list-style-type: none"> <li>a. Click .</li> <li>b. In the New Remote System Type dialog box, specify the details such as name, description, and version.</li> </ol>
Modify the protocol configuration of an existing remote system	<ol style="list-style-type: none"> <li>a. Select and double-click the remote system that you want to modify.</li> <li>b. Click .</li> </ol>

4. From the Connection Protocol list, select one of the following:
  - HTTPS with fallback to HTTP (default)
  - HTTPS only

- HTTP only

- Custom

5. Specify the details for the protocol, default port, and default timeout.

6. Click **Save**.

## Copyright information

Copyright © 2024 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

## Trademark information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.