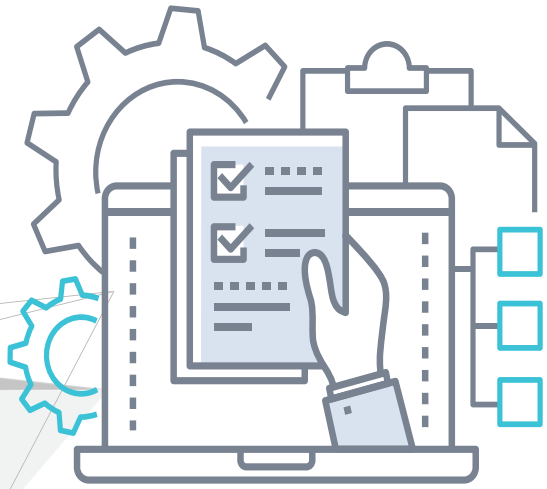
UNITRENDS

Deployment Guide for Unitrends Backup in Amazon Web Services

Release 10.9 | Document Date 07152025



Copyright

Copyright © 2025 Unitrends Incorporated. All rights reserved.

Content in this publication is copyright material and may not be copied or duplicated in any form without prior written permission from Unitrends, Inc (“Unitrends”). This information is subject to change without notice and does not represent a commitment on the part of Unitrends.

The software described in this publication is furnished under a license agreement or nondisclosure agreement. The software may be used or copied only in accordance with the terms of the license agreement. See the End User License Agreement before using the software.

The software described contains certain open source components that are copyrighted. For open source licenses, see the UnitrendsOpen Source Compliance section of the product Administrator Guide.

Because of the nature of this material, numerous hardware and software products are mentioned by name. In most, if not all, cases these product names are claimed as trademarks by the companies that manufacture the products. It is not our intent to claim these names or trademarks as our own.

The following applies to U.S. Government End Users: The Software and Documentation are “Commercial Items,” as that term is defined at 48 C.F.R.2.101, consisting of “Commercial Computer Software” and “Commercial Computer Software Documentation,” as such terms are used in 48 C.F.R.12.212 or 48 C.F.R.227.7202, as applicable. Consistent with 48 C.F.R.12.212 or 48 C.F.R.227.7202-1 through 227.7202-4, as applicable, the Commercial Computer Software and Commercial Computer Software Documentation are being licensed to U.S. Government end users (a) only as Commercial Items and (b) with only those rights as are granted to all other end users pursuant to the terms and conditions herein. Unpublished-rights reserved under the copyright laws of the United States. Unitrends agrees to comply with all applicable equal opportunity laws including, if appropriate, the provisions of Executive Order 11246, as amended, Section 402 of the Vietnam Era Veterans Readjustment Assistance Act of 1974 (38 USC 4212), and Section 503 of the Rehabilitation Act of 1973, as amended, and the regulations at 41 CFR Parts 60-1 through 60-60, 60-250, and 60-741. The affirmative action clause and regulations contained in the preceding sentence shall be incorporated by reference.

The following applies to all contracts and subcontracts governed by the Rights in Technical Data and Computer Software Clause of the United States Department of Defense Federal Acquisition Regulations Supplement:

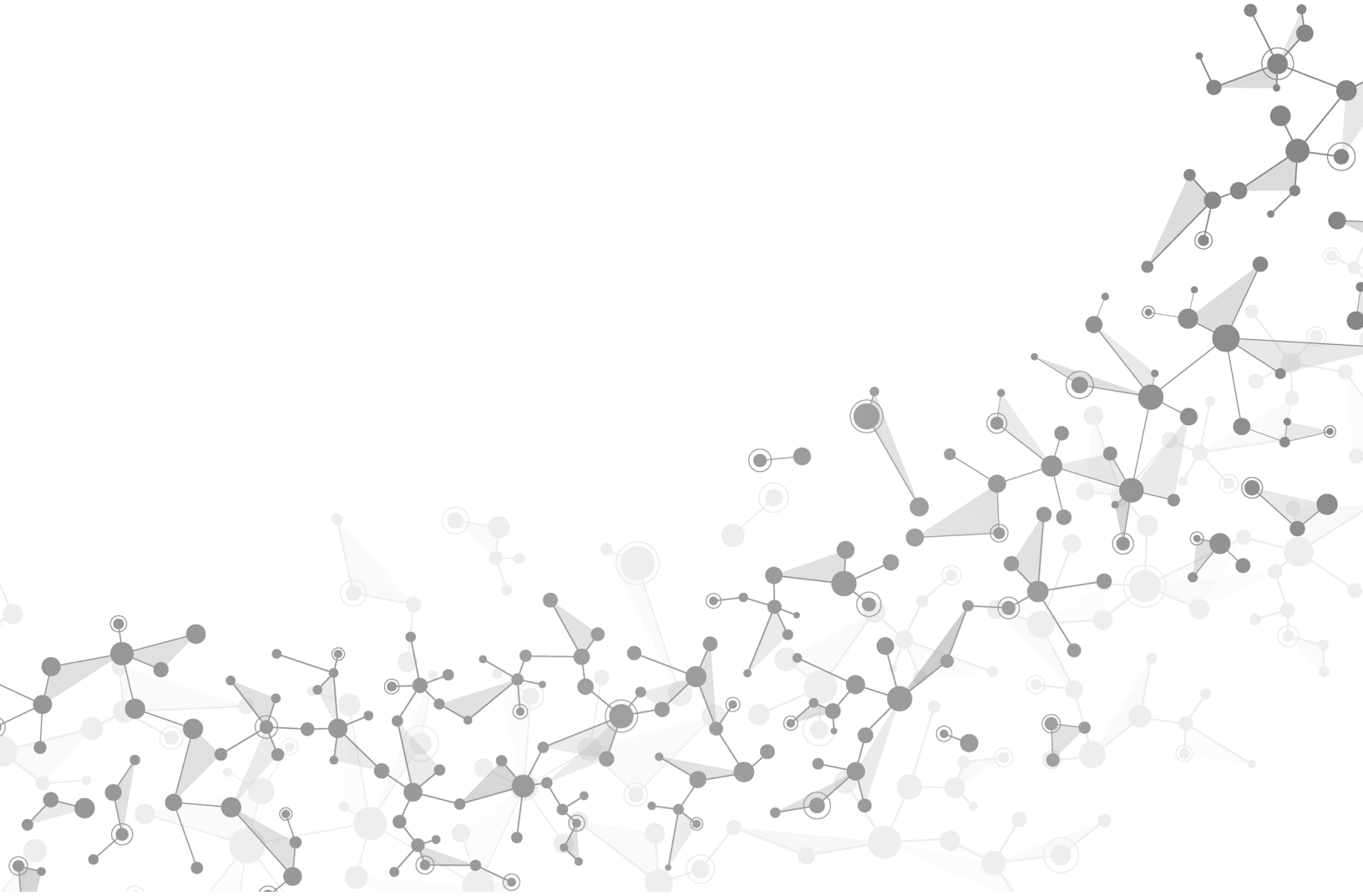
RESTRICTED RIGHTS LEGEND: USE, DUPLICATION OR DISCLOSURE BY THE UNITED STATES GOVERNMENT IS SUBJECT TO RESTRICTIONS AS SET FORTH IN SUBDIVISION (C)(1)(II) OF THE RIGHTS AND TECHNICAL DATA AND COMPUTER SOFTWARE CLAUSE AT DFAR 252-227-7013. UNITRENDS CORPORATION IS THE CONTRACTOR AND IS LOCATED AT 200 WHEELER ROAD, NORTH TOWER, 2ND FLOOR, BURLINGTON, MASSACHUSETTS 01803.

Unitrends, Inc
200 Wheeler Road
North Tower, 2nd Floor
Burlington, MA 01803, USA
Phone: 1.866.359.5411

Contents

Chapter 1: Introduction 5
Key Terms 5
Chapter 2: Requirements and Considerations 7
Network and web access requirements 7
Minimum resource requirements 7
Additional considerations 8
Limitations 8
Licensing 8
Chapter 3: Deploying the Unitrends Backup Instance 9
Step 1: Create the SSM IAM role 9
Step 2: Create the IAM Security Group 12
Step 3: Create the Unitrends Backup Instance 14
Step 4: Set up the appliance using the Quick Setup Wizard 15
Step 5: (If needed) Configure the Unitrends Backup appliance to use port 587 for SMTP 20
Step 6: Register and license the appliance 20

This page is intentionally left blank.



Chapter 1: Introduction

Unitrends Backup in Amazon Web Services leverages Unitrends Backup appliance technology as a deployable instance in Amazon's Elastic Compute Cloud. Our Amazon EC2-based Unitrends Backup Instance can be used as either a backup appliance or a backup copy target.

This deployment guide provides requirements, considerations, and instructions for deploying a Unitrends Backup appliance in Amazon's Elastic Compute Cloud.

For requirements and considerations for particular features and instructions on using them, see the Administrator Guide for Recovery Series, Recovery MAX, ION/ION+, and Unitrends Backup.

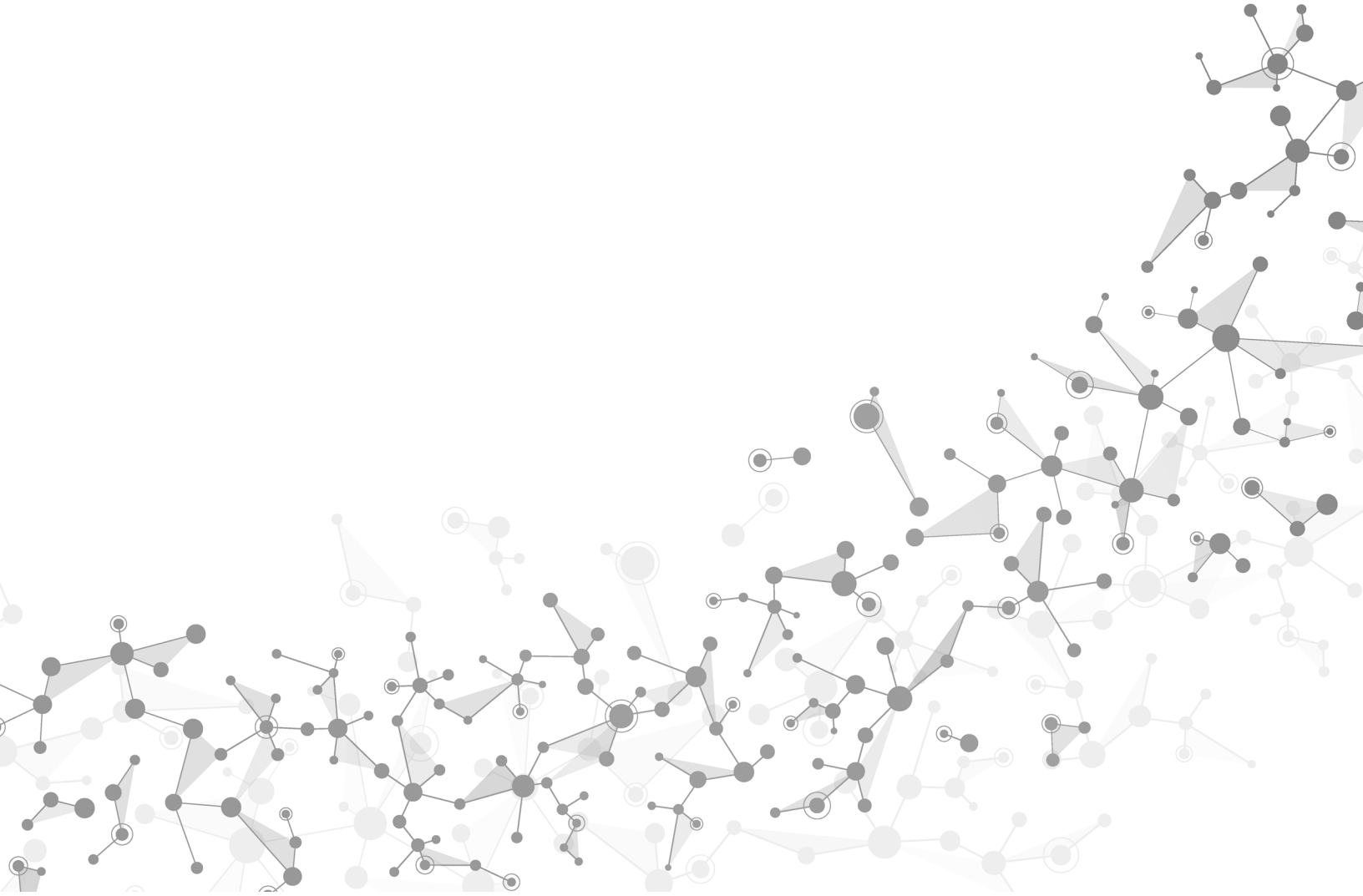
See the following topics for details on deploying the Unitrends Backup appliance:

- "Requirements and Considerations" on page 7
- "Deploying the Unitrends Backup Instance" on page 9

Key Terms

Term	Definition
AMI	Amazon Machine Image. The template that instances are launched from.
Appliance	The Unitrends Backup system that backs up and recovers data.
Deployment	The process of creating a Unitrends Backup Instance and configuring the appliance contained within.
Graphical User Interface	The browser-based user interface used for all normal appliance operations.
Quick Setup Wizard	The Quick Setup Wizard automatically launches the first time you access the appliance UI from a web browser. Work your way through this wizard to configure additional appliance settings, such as date and time, hostname, and email.
Root Volume	The volume that contains Unitrends Backup appliance system information.
Unitrends Backup Instance	An Amazon EC2 virtual machine that contains a Unitrends Backup appliance.

This page is intentionally left blank.



Chapter 2: Requirements and Considerations

Before deploying your Unitrends Backup appliance, review the following requirements:

- "Network and web access requirements"
- "Minimum resource requirements" on page 7
- "Additional considerations" on page 8
- "Limitations" on page 8
- "Licensing" on page 8

Network and web access requirements

The Unitrends Backup Instance's IAM Security Group (virtual firewall) must be configured to meet the inbound and outbound rules described in "Create the IAM Security Group" on page 12. These rules are needed for:

- Connectivity between the appliance and its protected assets
- Connectivity between the appliance and the Internet
- Connectivity between the appliance and your SMTP server
- Connectivity between the appliance and its hot backup copy target (required only if you are running hot backup copies)

IMPORTANT! Never expose the appliance Web UI or SSH connections to open external ports. Doing so may void your support agreement until the appliance can be secured properly. Never deploy the Unitrends appliance on a public IP. All incoming ports to a Unitrends appliance must be firewall protected. Privately operated hot backup copy targets should be deployed in such a way as to secure the VPN connection to only trusted source external IPs.

Minimum resource requirements

To ensure successful deployment, the Unitrends Backup instance must be deployed as an Amazon EC2 instance type that meets or exceeds the following specifications:

Note: These are the minimum resources required to deploy and begin using the Unitrends Backup appliance. As you add jobs and storage, be sure to monitor the system and add resources as needed over the lifetime of the appliance.

- A minimum of two virtual processors (vCPUs).
- A minimum of 8GiB of memory.
- A root volume of exactly 100GiB.
- An EBS volume of at least 250GiB for backup data storage.

Additional considerations

- A Unitrends Backup Instance must be deployed in the same region and subnet as the Amazon EC2 assets it is protecting.
- To use the hot backup copy feature, the source Unitrends Backup Instance and target Unitrends Backup Instance must be deployed in the same region and subnet .
- After deploying your Unitrends Backup appliance, you will perform all operations, including updates, from the web UI.
- By default, the password for the web UI root user of the Unitrends appliance is *unitrends1*. You will change this password during appliance setup, as described in "Set up the appliance using the Quick Setup Wizard" on page 15.
- By default, the password for the appliance OS root user is *unitrends1*. You will change this password during appliance setup, as described in "Set up the appliance using the Quick Setup Wizard" on page 15.
- By default, appliance deduplication level is set to 1. For further information, see Managing Appliances in the Unitrends Backup and Recovery Series Administrator's Guide.
- As a matter of best practice, Unitrends recommends configuring a backup storage volume size of 1.5x the initial data set you are protecting. More storage can be added if you desire a longer data retention period.
- All additional backup storage volumes added to the Unitrends Backup Instance must be configured as EBS General Purpose SSD (GP2) volumes.

Limitations

The following limitations apply:

- The Unitrends Backup Instance must be in the same subnet as the amazon EC2 assets you wish to protect.
- If this Unitrends Backup Instance is slated for use as a backup copy target, it must be deployed in the same subnet as the appliance it will receive backups from.

The following Unitrends Backup features are not currently supported within the Amazon EC2 environment:

- Backups that are not agent-based application or file-level. (Host-level and image-level backups are not supported.)
- Bare metal recovery.
- Instant Recovery.
- Using a physical seed device to move data into or out of the Amazon EC2 environment.
- Exporting a Unitrends Backup appliance to a host outside of the Amazon EC2 environment.

Licensing

You must register and license the appliance after deploying your Unitrends Backup appliance. You can use the software for free with a 30-day trial license, but after this period, you must purchase a license.

Chapter 3: Deploying the Unitrends Backup Instance

Once you have verified that all requirements have been met, complete the following steps to deploy the Unitrends Backup Instance:

Step 1: "Create the SSM IAM role"
Step 2: "Create the IAM Security Group"
Step 3: "Create the Unitrends Backup Instance "
Step 4: "Set up the appliance using the Quick Setup Wizard" on page 15
Step 5: "(If needed) Configure the Unitrends Backup appliance to use port 587 for SMTP" on page 20
Step 6: "Register and license the appliance" on page 20

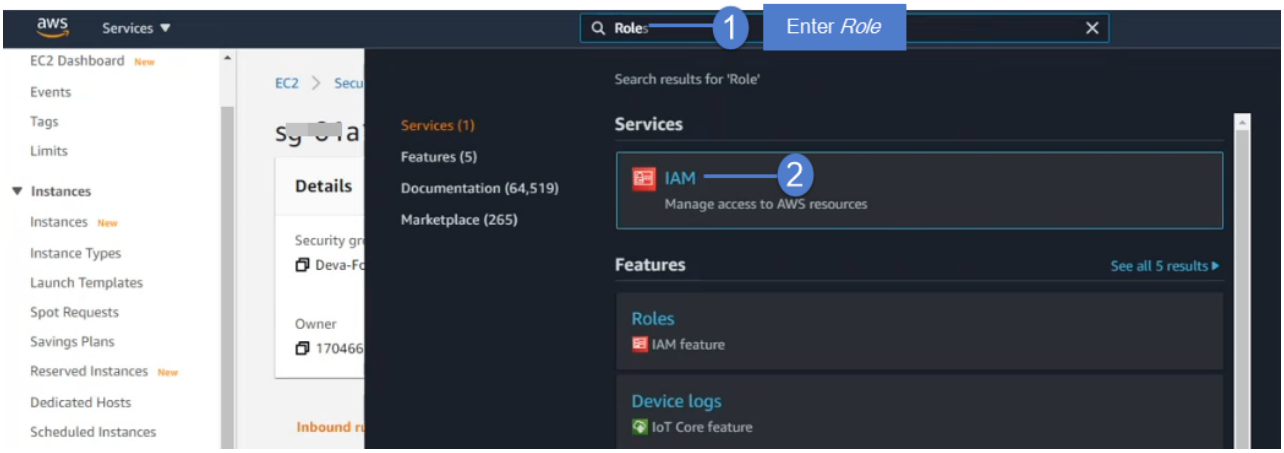
Step 1: Create the SSM IAM role

Use this procedure to create the IAM role that AWS Session Manager uses to access the appliance command line.

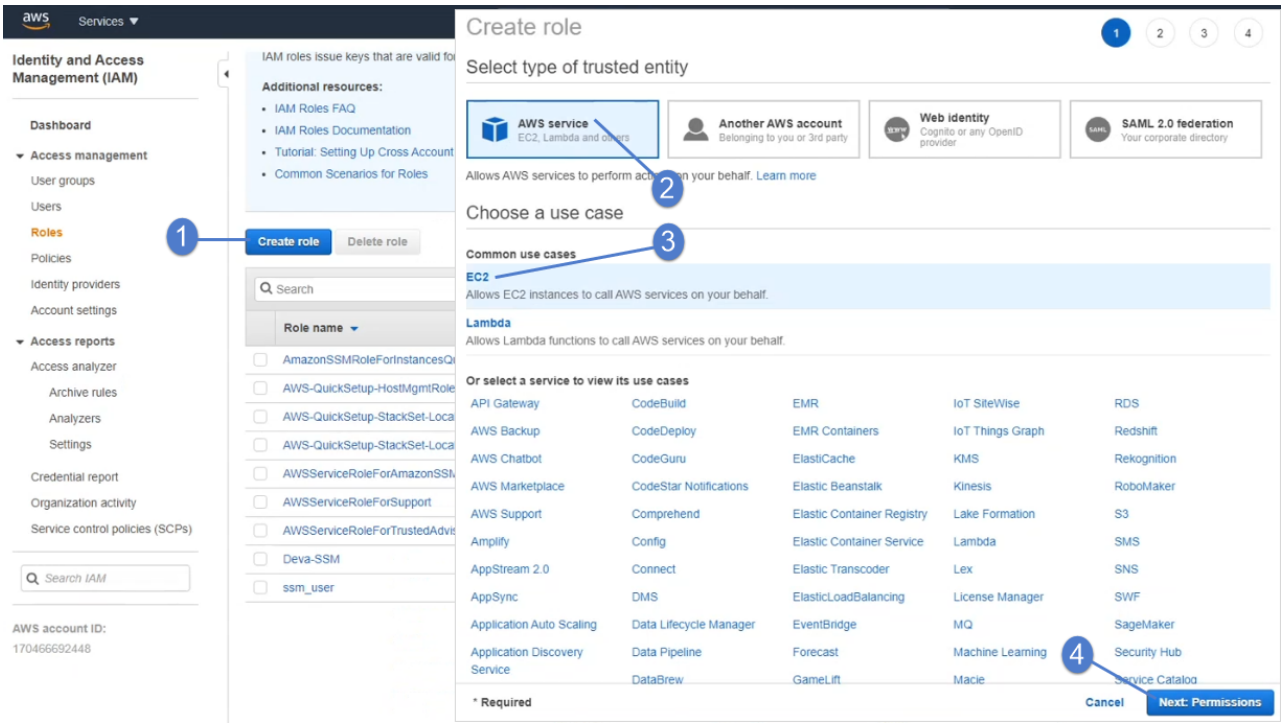
> **Note:** Appliance administration tasks are run from the appliance UI. In some cases, Support may need access to the command line for advanced troubleshooting. The role you create using this procedure is needed to enable command line access via AWS Session Manager.

From the AWS Management Console (**EC2 > Launch Instance**):

1. In the Search field, enter *Role*, then select **IAM**.

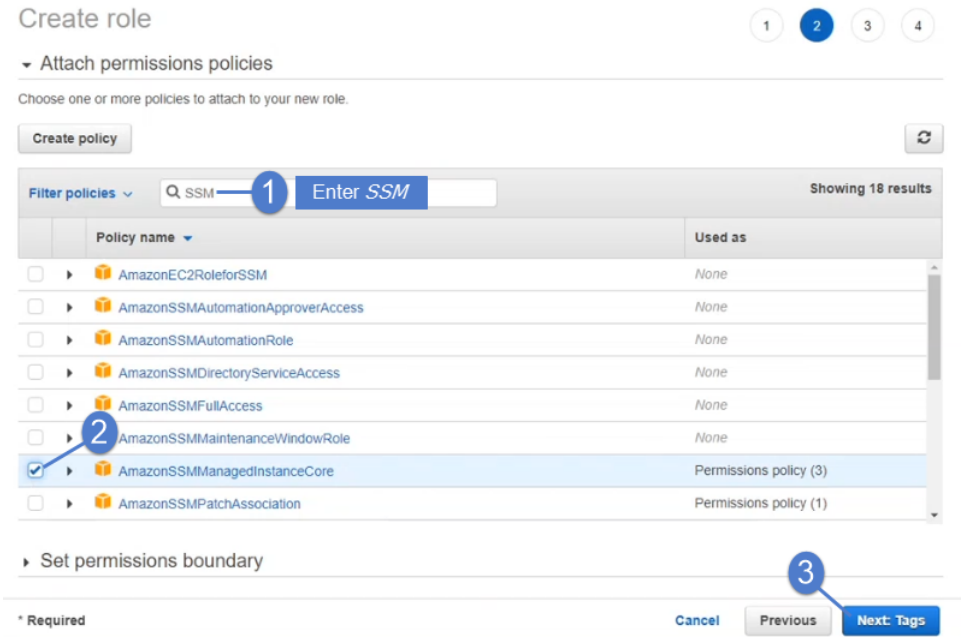


2. Click **Create Role**.
3. Select the **AWS Service** type and **EC2** use case.
4. Click **Next: Permissions**.

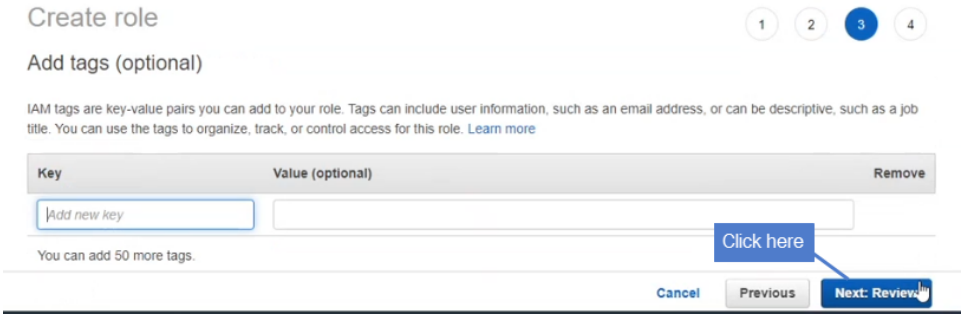


5 In the Search field, enter *SSM*, then select **AmazonSSMManagedInstanceCore**.

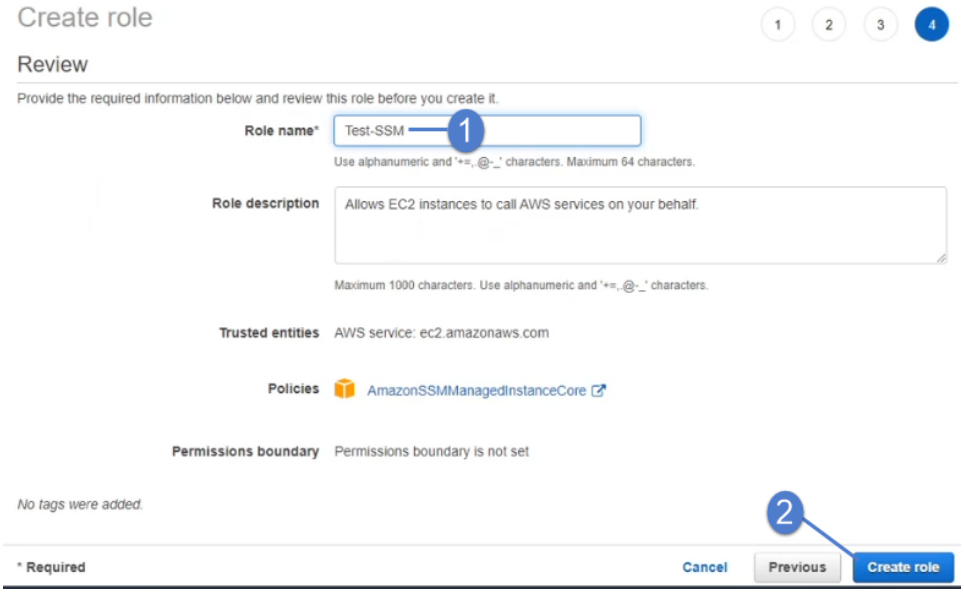
6 Click **Next: Tags**.



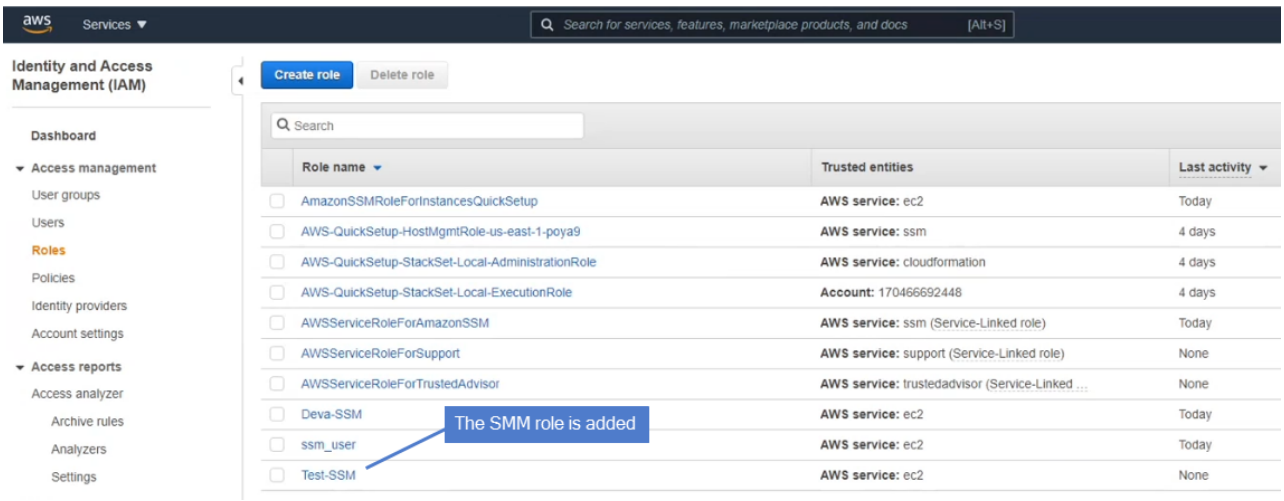
7 (Optional) Add tags. Click **Next Review**.



8 Enter a Role Name. Click **Create Role**.



The role is created.



Step 2: Create the IAM Security Group

Configure the Unitrends Backup Instance's IAM Security Group (virtual firewall) to meet the inbound and outbound rules described below.

Inbound rules

The following inbound rules are required :

Notes:

- SSH access to the appliance command line is not permitted. For increased security, you must block inbound access to port 22 on the Unitrends Backup Instance. Do not add port 22 to the security group's inbound rules.
- Most appliance administration tasks can be done through the appliance UI. If you are working with Support and need command line access, connect by using the AWS Session Manager.

Inbound Rules				
Type	**Protocol**	**Port range**	**Source**	**Notes**
All traffic	All	All	Do one of the following: • If you are editing an existing security group, enter the security group name. Or • If your creating a new security group, create the security group without adding the *All traffic* rule. Once the security group is created, edit the group to add the *All traffic* rule with the security group name in the Source field.	Enables communication between all instances in the security group.
Custom TCP	TCP	443	0.0.0.0/0	Configure the Source as a trusted IP address.

Outbound rules

By default, AWS allows all traffic in outbound rules. If you do not want to allow all traffic, the following outbound rules are required:

Outbound Rules				
Type	**Protocol**	**Port range**	**Source**	**Notes**
Custom TCP	TCP	443	74.202.224.68/32	IP address of support-itivity.unitrends.com, which enables remote support. Used for opening a remote tunnel to the Unitrends support team.
Custom TCP	FTP	20 and 21	52.90.71.124/32	IP address of repo.unitrends.com, which is used by the Unitrends appliance to perform software updates.
Custom TCP	HTTP	80	34.229.183.15/32	IP address of ftp.unitrends.com, which is used by Support to install patches and updates.
Custom TCP	TCP	161 and 162	104.130.228.89/32	IP address of notifications.unitrends.com. Used for proactive monitoring through SNMP trap collection.
Custom UDP	UDP	161 and 162	104.130.228.89/32	IP address of notifications.unitrends.com. Used for proactive monitoring through SNMP trap collection.
Custom TCP	TCP	587 **Note:** Use port 587 unless your SMTP server must be configured to listen on port 25.	IP address of the SMTP server.	Used for connectivity between the Unitrends Backup Instance and your SMTP server. Additional SMTP setup is required. See "SMTP setup" for details.
Custom TCP	TCP	The port number you have configured for the secure tunnel connection to the backup copy target appliance.	Private IP address of the target Unitrends Backup appliance (the appliance that is receiving backup copies).	This outbound rule is required for hot backup copy. This rule is not needed if you are not copying backups to a second appliance.

Outbound Rules				
Type	Protocol	Port range	Source	Notes
Custom TCP	TCP	443	Private IP address of the target Unitrends Backup appliance (the appliance that is receiving backup copies).	This outbound rule is required for hot backup copy. This rule is not needed if you are not copying backups to a second appliance.

SMTP setup

Configure your SMTP server and IAM security group to use port 587 unless your SMTP server is required to listen on port 25.

- Port 587 – To use port 587, add the port your outbound rules. After you deploy the Unitrends Backup Instance, you will configure the appliance to use port 587 for SMTP (as described in "Step 5: (If needed) Configure the Unitrends Backup appliance to use port 587 for SMTP".)
- Port 25 – AWS blocks port 25 by default. If you must use this port for SMTP, send AWS a request to open port 25. For details, see this AWS article: How do I remove the restriction on port 25 from my Amazon EC2 instance or AWS Lambda function?

Step 3: Create the Unitrends Backup Instance

From the AWS Management Console (**EC2 > Launch Instance**):

1. Choose **AMI**. Select **Community AMIs**. Search for and select **Unitrends Backup**.
2. Choose an Instance type. Click **Next**.

   WARNING! To deploy successfully, you must select an instance type that meets or exceeds the minimum specifications of 2 vCPUs and 8GiB of memory.

3. Configure the Instance. Click **Next**.
   - Number of instances – Configure as desired.
   - Purchasing option – This is optional.
   - Network – You may select the default network or create a new one.
   - Subnet – This must be the same subnet as the Amazon EC2 assets you wish to protect.

     If this Unitrends Backup Instance is slated for use as a backup copy target, it must be deployed in the same subnet as the appliance it will receive backups from.
   - Auto-assign public IP – This must be enabled.
   - IAM role – Assign the SSM role you created above in Step 1:
   - Shutdown behavior – Select **Stop**.

- Enable termination protection – This is strongly recommended.
- Monitoring – This is optional.
- Tenancy – Configure as desired.
- Advanced Details – Configure as desired.

4 Add storage. Click **Next**.

- Configure the root volume as a 100GiB General Purpose SSD (GP2). This volume will be used for appliance system data. Do not select the Delete on Termination option.
- Add a new EBS volume and configure it as General Purpose SSD (GP2) of at least 250GiB. This volume will be used to store backup data.
  - Do not select the Delete on Termination option.
  - Do not Encrypt this volume.

5 (Optional) Add Tags. Click **Next**.

6 Add the security group you configured above in Step 2: Click **Review and Launch**.

7 Review the settings. If you are satisfied with the configuration of your instance, click **Launch**.

8 Click **Launch Instances**.

Step 4: Set up the appliance using the Quick Setup Wizard

After the EC2 Management Console indicates the instance is running, you can access the appliance UI from any machine on the same network by opening a Chrome or Firefox browser and entering the appliance's private IP address followed by */ui/*, or from outside of the network by entering the appliance's public IP address followed by */ui/*. In most cases, this automatically logs you in to the UI. If the login screen displays, enter the following default credentials to log in to the appliance UI for the first time:

Username: *root*

Password: *unitrends1*

The Quick Setup Wizard launches when you access the UI for the first time.

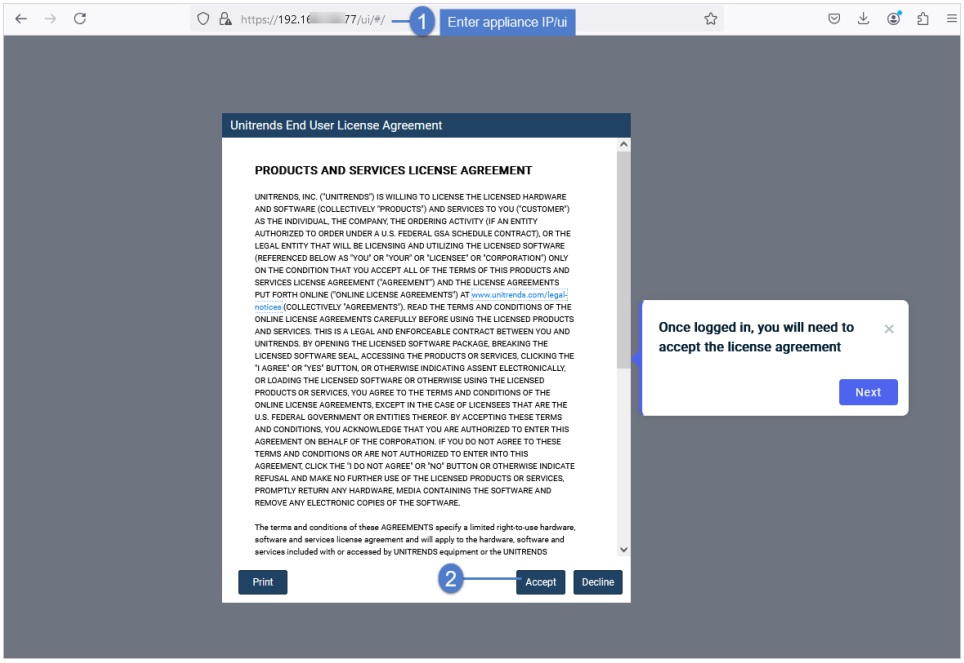
Note: The Unitrends Backup instance may require 5 to 15 minutes to boot.

To set up the appliance

Use this procedure to set up the appliance:

1 Open a browser and connect to your appliance by entering: ***https://<applianceIP>/ui***. For example: ***https://10.10.10.1/ui***.

2 Click **Accept** to accept the license agreement.

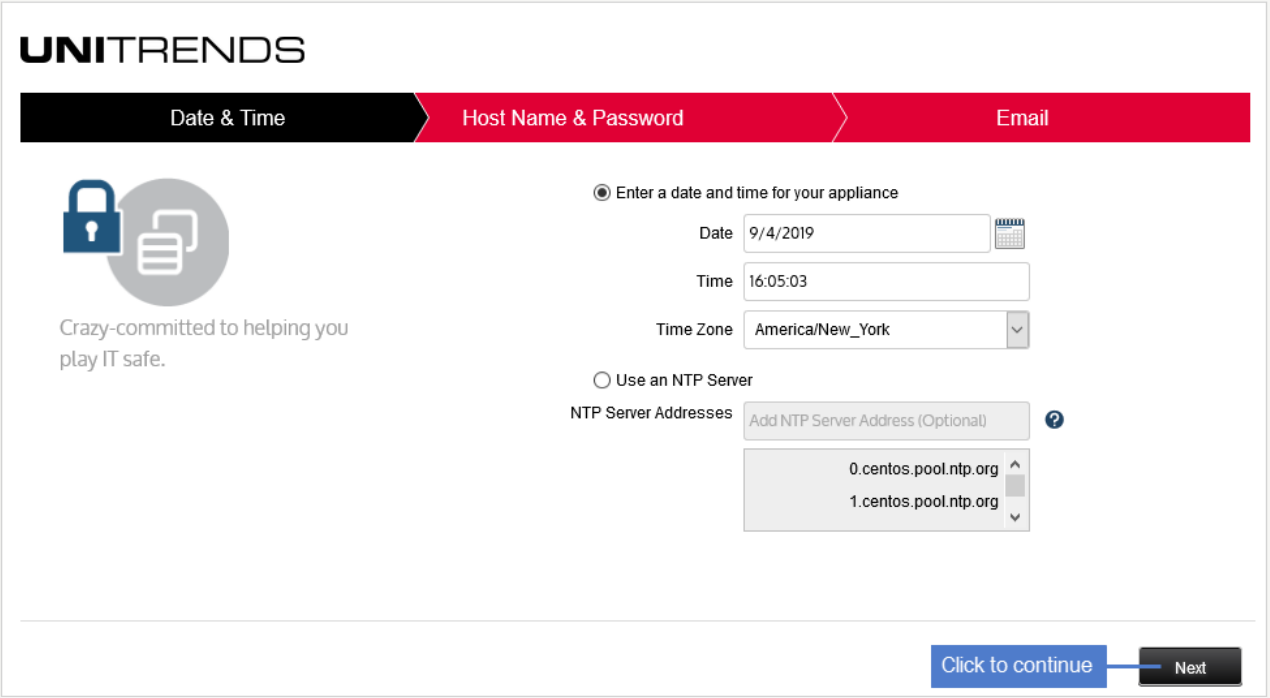


3 Set the appliance date and time by doing one of the following, then click **Next**:

- Select a **Timezone**. If needed, modify the appliance **Date** and **Time**.

OR

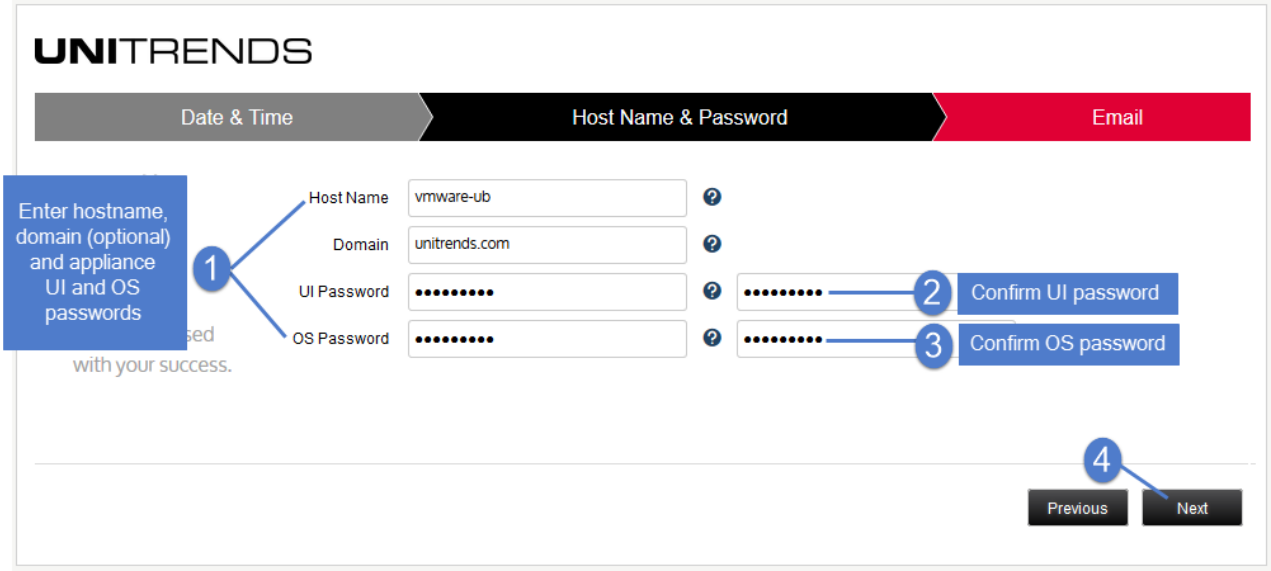
- Check the **Use an NTP Server** box to sync to an NTP server. (Optional) Enter your preferred NTP server address.



4 Enter a **Host Name**, a **Domain**, a new **UI Password**, and a new **OS Password** for the appliance. Confirm the passwords by entering them again in the fields to the right. Click **Next**.

Notes:

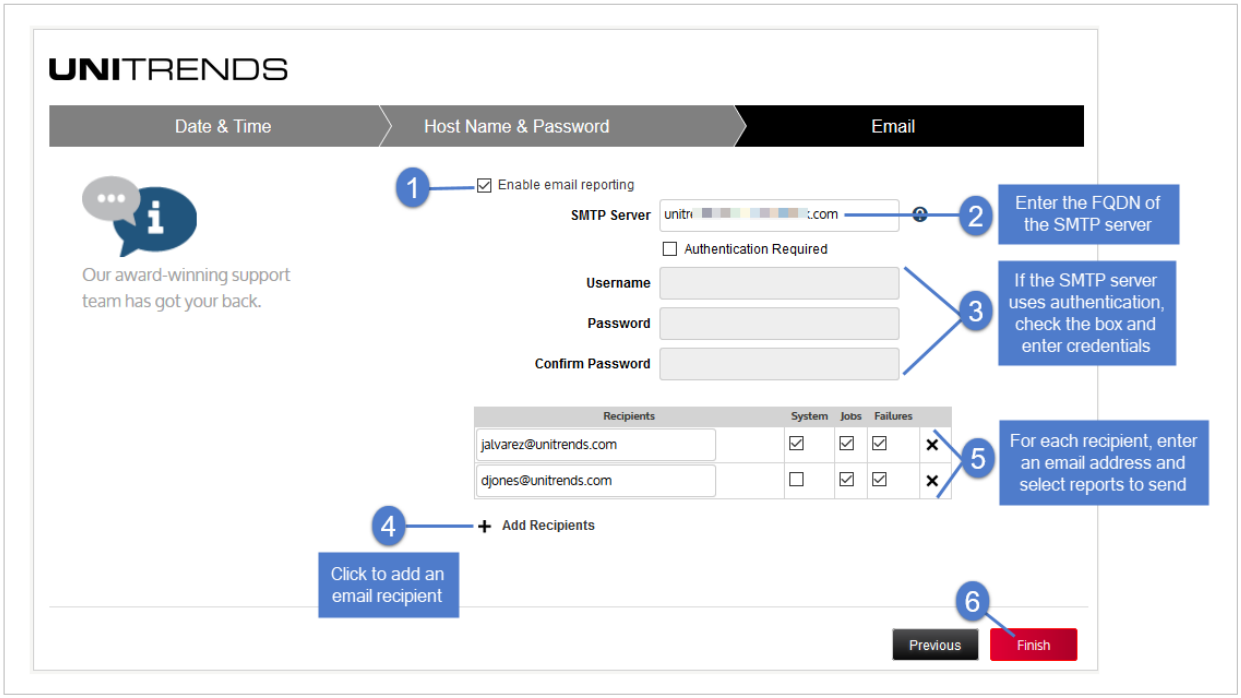
- The hostname can contain only alphanumeric characters, dashes, and underscores.
- The appliance has a UI root user and an OS root user. These are separate accounts. Changing the password of one root user account does NOT change the password of the other root user account.
- Passwords cannot contain the word *Unitrend* (case insensitive).
- The OS password must contain 8 or more characters.
- All appliances are deployed with these default UI and OS credentials: user *root*, password *unitrends1*. For appliance security, you must change these passwords in the Quick Setup Wizard. For increased security, ensure that the OS password you enter is different than the UI user password.
- After you finish the deployment procedures in this guide, you can set up additional UI users for the appliance at any time. For details, see *Users and roles* in the Administrator Guide for Recovery Series, Recovery MAX, ION/ION+, and Unitrends Backup, Appliance settings topic.



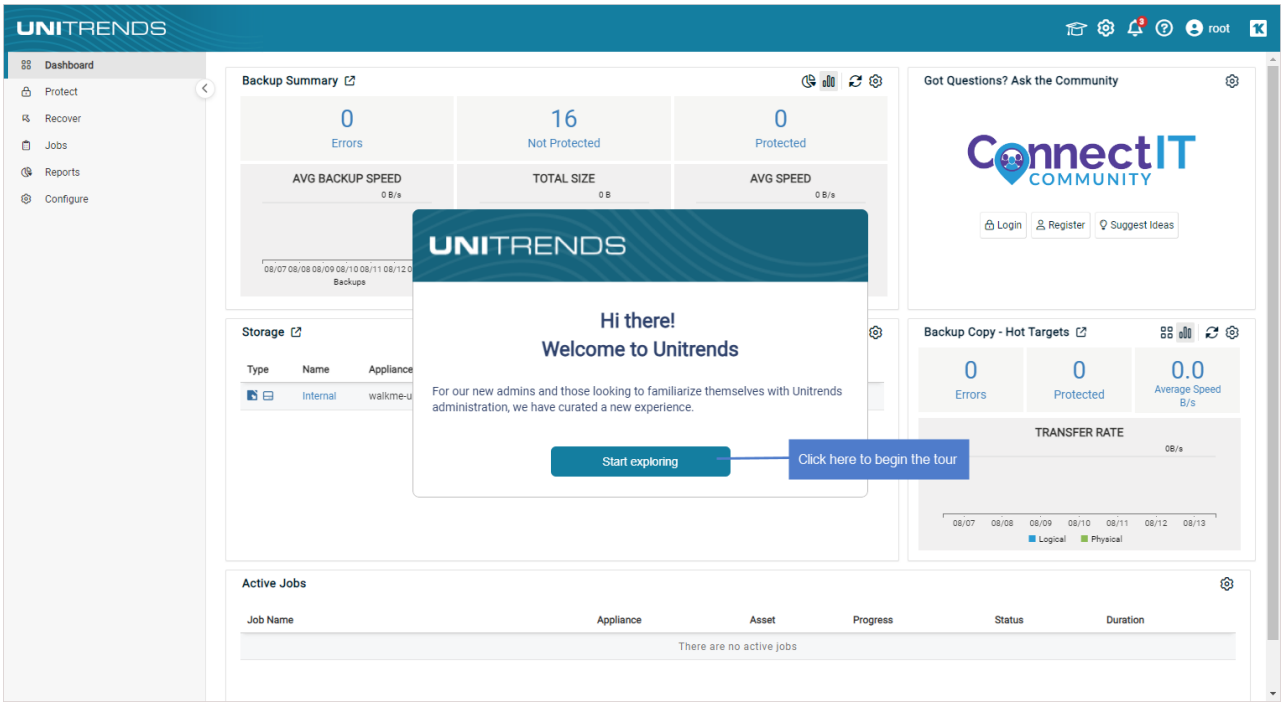
5 (Optional) To enable email from the appliance, check **Enable email reporting** and enter the following:

- The fully qualified domain name of the **SMTP server**.
- (If needed) If the SMTP server requires authentication, select **Authentication required** and enter a **Username** and **Password**.
- Click **+ Add Recipients** to add a an email recipient. Enter an email address in the **Recipient** field and select one or more of the **System**, **Jobs**, and **Failures** options to specify which reports the appliance will send to the recipient. Repeat as needed to add more recipients.

6 Click **Finish**.



The Welcome to Unitrends dialog displays. Click **Start exploring** to view the interactive product tour. Then proceed to the next step in this procedure.



7 Configure appliance DNS settings:

- On the **Configure > Appliances** page, select the appliance and click the **Network** tab.
- Select the desired adapter and click **Edit**.
- Verify the IP address of the **Preferred DNS** server is correct.
- Enter the IP address of the **Alternate DNS** server (optional), and the **DNS Search** domain, then click **Save**.

8 Expand primary backup storage in the Unitrends Backup UI:

WARNING! Once a disk has been expanded as primary backup storage, it cannot be removed.

- Log in to your Unitrends Backup virtual appliance.
- On the **Configure > Appliances** page, select your appliance.
- Click the **Storage** tab.
- Select the **Internal** storage and click **Edit**.
- In the Manage Attached Disks area:
  - To add an attached disk, select the desired disk from the list of available attached disks and click **Add**.
  - To remove an attached disk from the list, select it from the list of available attached disks and click **Remove**.
  - Clicking **Reset** reverts all disk settings to the original settings.
  - To refresh the list of available disks, click **Refresh**.
- Click **Save**.
  On the **Configure > Appliances** page, the status initially displays as *Pending*. When the disk is finished attaching, the status converts to *Active* and the storage can be used.
- If desired, repeat this procedure to add another disk.

Step 5: (If needed) Configure the Unitrends Backup appliance to use port 587 for SMTP

Run the procedure in AWS Email Notifications setup for port 587 if you are using port 587 for SMTP. Do not do this step if you are using port 25.

Step 6: Register and license the appliance

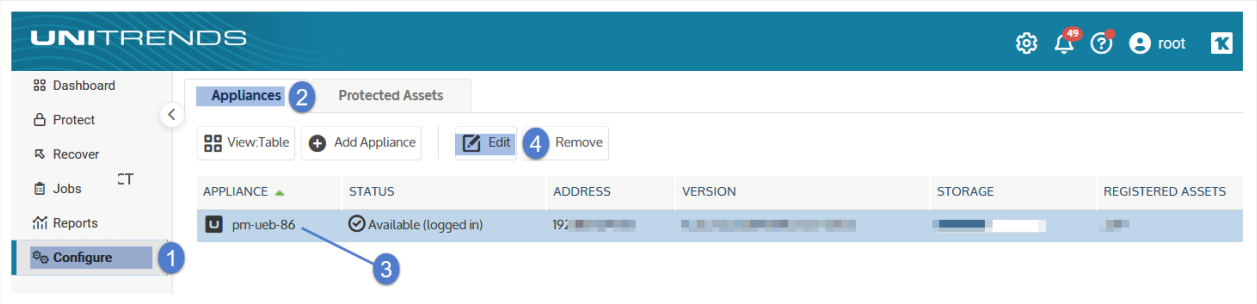
Your appliance is now configured and you can begin using it to protect your environment. For details, see the Administrator Guide for Recovery Series, Recovery MAX, ION/ION+, and Unitrends Backup.

You must register and license the appliance within 30 days of deploying Unitrends Backup.

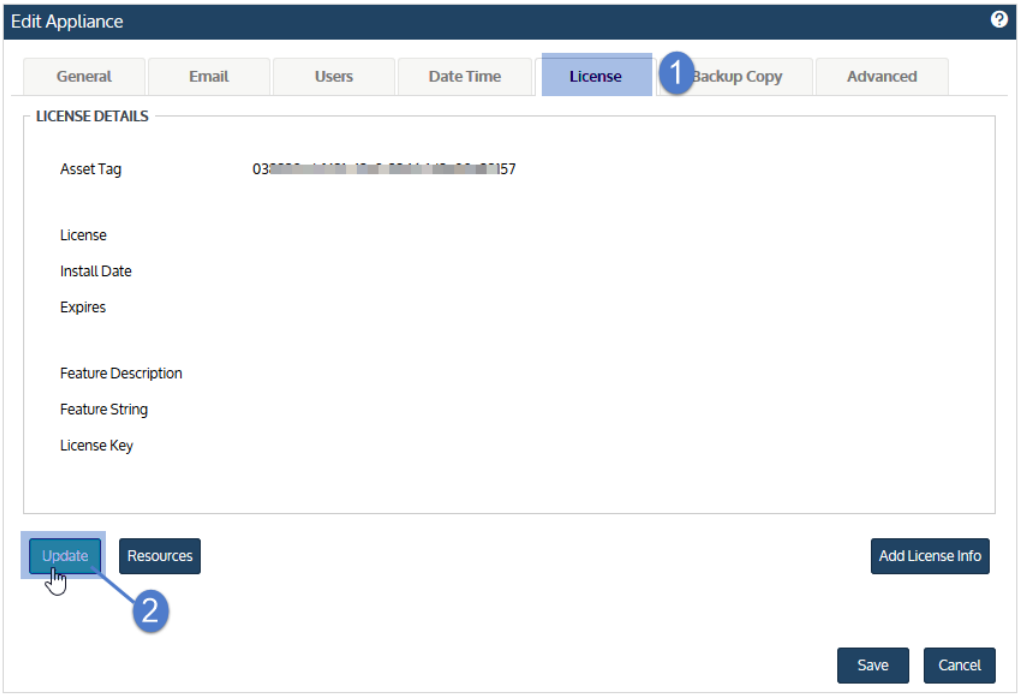
Each appliance requires an activation code and license key. Use the procedures below to register and license the appliance:

To register a Unitrends Backup appliance

1 On the **Configure > Appliances** page, select the appliance and click **Edit**.



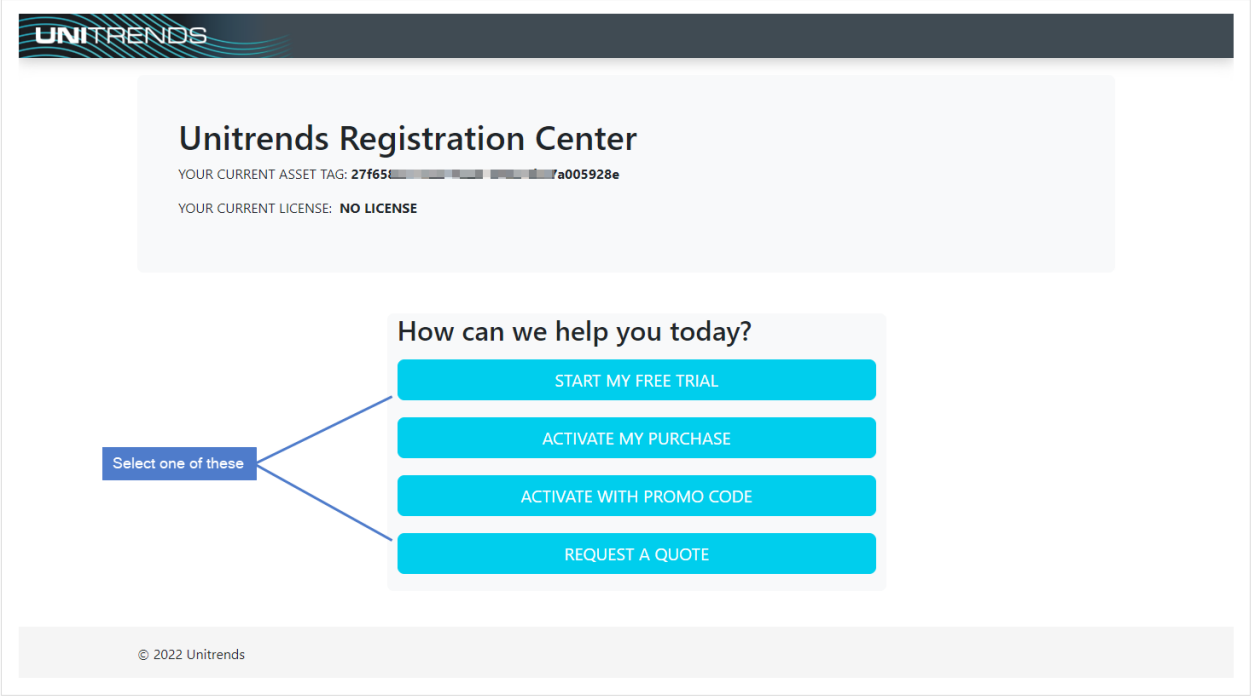
2 Select the **License** tab and click **Update**. The Registration Center displays.



3 Select one of the following:

Selection	Description
Start my free trial	Submit this form to start your free 30-day trial.
Activate my purchase	Enter your email address and activation code. You license key will be emailed to the address you enter here.
Activate with promo code	Enter your promotional code to register your product and receive your license key.

Selection	Description
Request a quote	Request a license quote.



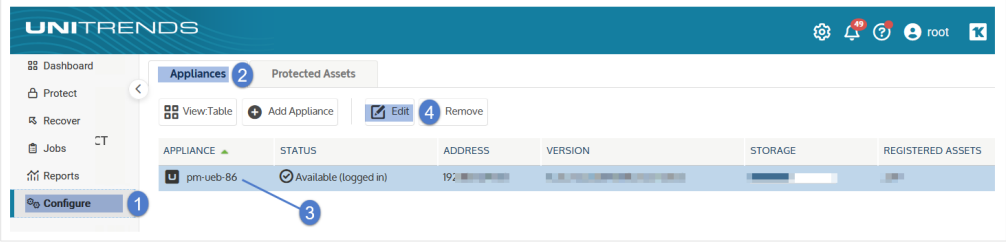
4 Complete and submit the applicable form.

Once you have purchased a license, Unitrends sends an email containing license details. Use the next procedure to apply this license information to the appliance.

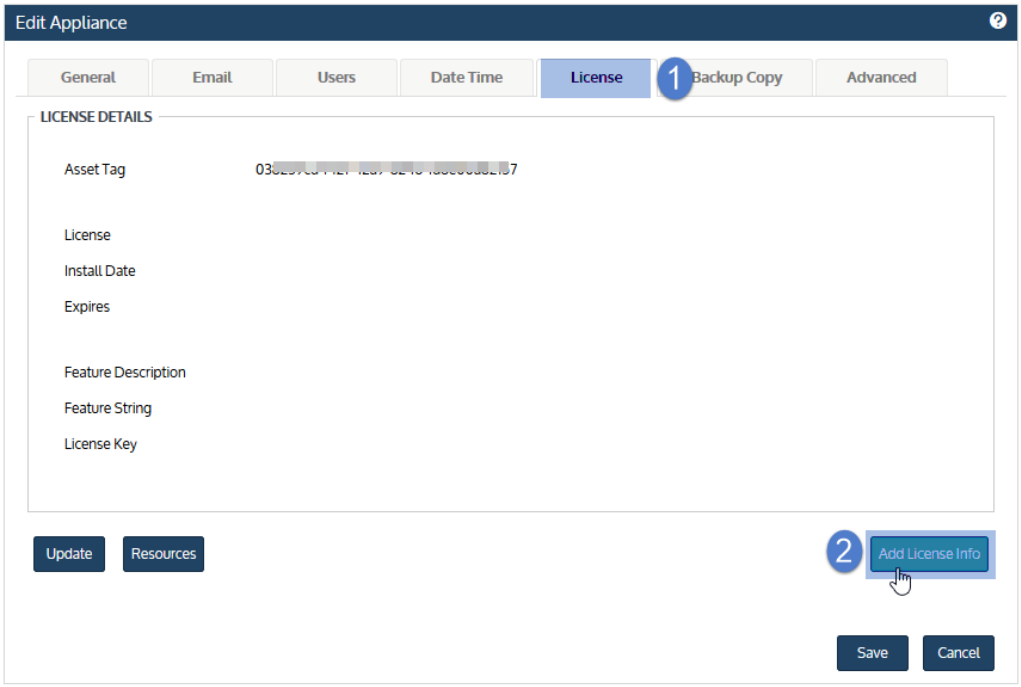
To license a Unitrends Backup appliance

Use these steps to enter license information you have received from Unitrends.

1 On the **Configure > Appliances** page, select the appliance and click **Edit**.

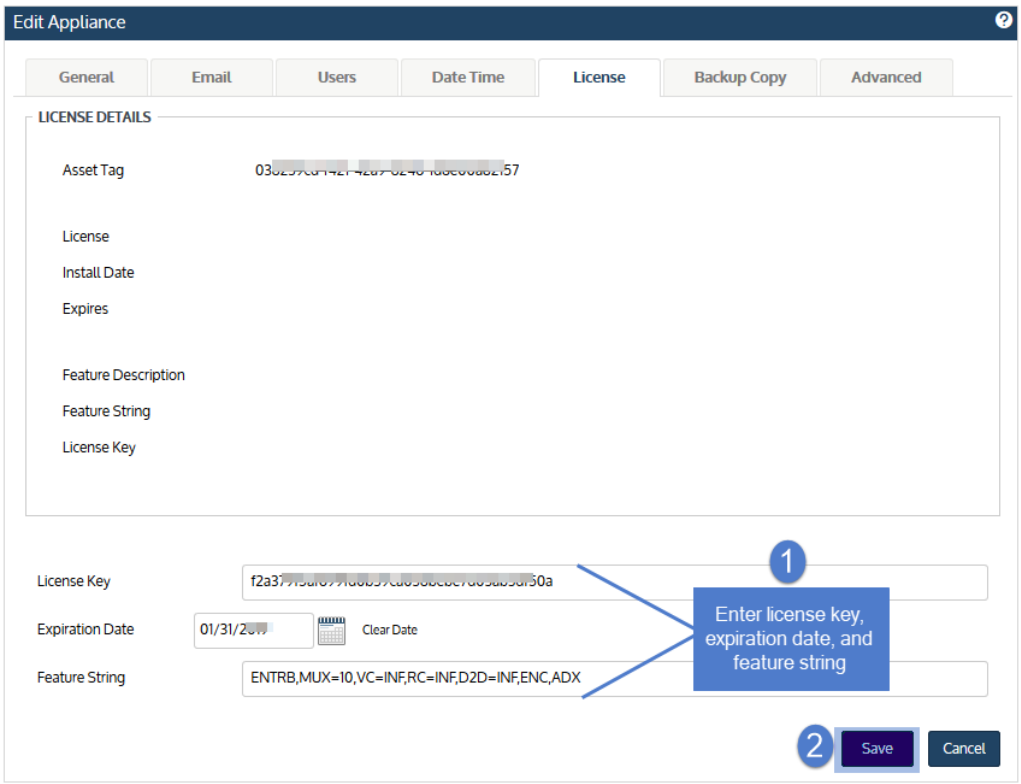


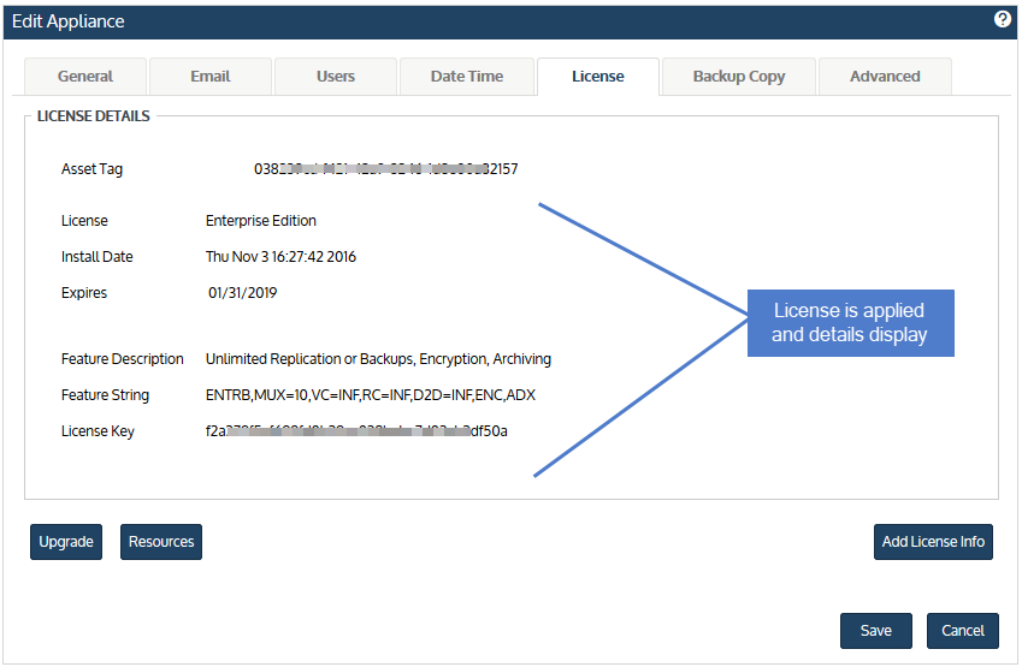
2 Select the **License** tab and click **Add License Info**.



3 Enter the **License Key**, **Expiration Date**, and **Feature String**.

4 Click **Save**. The license is applied.




Edit Appliance
General
Email
Users
Date Time
License
Backup Copy
Advanced
LICENSE DETAILS
Asset Tag
License
Enterprise Edition
Install Date
Thu Nov 3 16:27:42 2016
Expires
01/31/2019
Feature Description
Unlimited Replication or Backups, Encryption, Archiving
Feature String
ENTRB,MUX=10,VC=INF,RC=INF,D2D=INF,ENC,ADX
License Key
License is applied and details display
Upgrade
Resources
Add License Info
Save
Cancel