



Teramind on AWS

Deployment Guide

Ver 7.4 (11 APR 2024)



Table of Contents

Teramind on AWS Overview	2
Benefits of Deploying Teramind on AWS.....	2
Primary Server Requirements	3
Database Server Requirements	4
OCR Server Requirements	5
Storage Requirements	6
Agent Requirements	7
Prerequisites.....	8
Creating an AWS Instance	9
Creating an RDS Database	14
Adding an S3 Storage	19
Finishing the Deployment	22
Setting up the OCR (optional).....	28
Installing the Teramind Agent	32
Firewall & Proxy Considerations	32
Antivirus Considerations	32
Additional Configurations	33
Changing the License Key.....	33
Updating the Server	33
Setting Up the Active Directory / LDAP Integration.....	33
SMTP Email	34
SSL Certificate	34
Architecture.....	35
Technical Specifications	36
Installation Support and Troubleshooting	37

Teramind on AWS Overview

All Teramind solutions are available to deploy on Amazon’s distributed, highly scalable, and reliable Amazon Web Services (AWS) platform as a Private Cloud option. This deployment guide will help you discover what you can expect from your Teramind on AWS deployment and provide you with installation prerequisites, step-by-step instructions, technical and support information.

Benefits of Deploying Teramind on AWS

If you prefer on-premise deployments but unwilling to incur the cost and hassle of an in-house infrastructure or you want to move to the Cloud but have been concerned about compliance, security or have made the transition and already host on AWS, then Teramind on AWS is the right choice for you. With our AWS Private Cloud hosting option, enjoy the benefits of both worlds: cost and scalability comparable to a Cloud deployment and security and flexibility similar to an On-Premise solution. Here are some infrastructure benefits you can expect if you choose to deploy Teramind on AWS:



Flexible and Competitive Pricing

You only pay for the AWS resources you consume (i.e. CPU, storage, memory). Teramind’s recommended configuration for a standard deployment (*m4.xlarge* instance, supporting up to 100 users) costs only a few cents per hour*.

**Infrastructure costs are set by Amazon and subject to change.*



Optimized Environment

Choose the region, OS, storage, database, etc. For example, you can use an Amazon S3 storage for Teramind’s session recordings and Amazon RDS databases for session logs that are highly optimized for performance on AWS.



Easy Deployment

Create a Teramind server with a single click by launching the Teramind AMI (Amazon Machine Image) from the AWS Marketplace.



Reliability

Support for High Availability (HA), redundancy with multi-geo replications, on-demand backup, and disaster recovery.



Scaling

Vertical and horizontal scaling with optional auto-scaling that adjusts capacity based on demand.



Central Management Console

Configure and manage all your deployments from one central location.



Security and Compliance

Firewall, encryption at rest, SSL encryption, VLAN, SSH tunnels, 2FA, IP whitelisting, and encrypted disks allowing for easy regulatory compliance for HIPAA, GDPR, PCI DSS, and more make it ideal for Teramind customers in government, healthcare, finance, and other regulated industries.

Primary Server Requirements

Deployments for under 1,000 concurrent users can be hosted on one all-inclusive server, in most cases. EC2 instance(s) should be provisioned based on the expected number of concurrent monitored sessions, according to the following table:

Concurrent Users*	Server Requirements	EC2 Instance Type
Up to 100	1 Teramind Master Server (VM)	<ul style="list-style-type: none">m4.xlarge
Up to 500	1 Teramind Master Server (VM)	<ul style="list-style-type: none">m4.2xlarge
Up to 1, 000	1 Teramind Master Server (VM)	<ul style="list-style-type: none">m4.4xlarge
Larger deployments: <i>1,000 or more concurrent users</i>	1 Teramind Master Server (VM)	<ul style="list-style-type: none">m4.4xlarge
	1 Teramind App Server (VM) per 1,000 concurrent users	<ul style="list-style-type: none">m4.4xlarge
	1 Teramind BI Server (VM)	<ul style="list-style-type: none">m4.4xlarge

*The requirements are applicable for a typical user who works on a single computer with Full HD (1920x1080) screen resolution, doing regular office work. If the users have multiple screens, higher-resolution screens, or have an unusual work pattern (e.g., watching many videos) then the requirements will be higher.

Database Server Requirements

Concurrent Users*	Server Type	CPU/RAM/Disk
Up to 100	db.t3.medium	<ul style="list-style-type: none">• CPU: 2 vCPU• RAM: 4 GB• Disk: 100 GB**
Up to 500	db.t3.xlarge	<ul style="list-style-type: none">• CPU: 4 vCPU• RAM: 16 GB• Disk: 500 GB**
Up to 1,000	db.t3.2xlarge	<ul style="list-style-type: none">• CPU: 8 vCPU• RAM: 32 GB• Disk: 1 TB**
Larger deployments: <i>1,000 or more concurrent users</i>	db.m4.4xlarge or more	<ul style="list-style-type: none">• CPU: 16 vCPU• RAM: 64 GB• Disk: 1 TB or more**

*The requirements are applicable for a typical user who works on a single computer with Full HD (1920x1080) screen resolution, doing regular office work. If the users have multiple screens, higher-resolution screens, or have an unusual work pattern (e.g., watching many videos) then the requirements will be higher.

**Disk size is estimated for 1 year of average usage and may vary depending on monitored data, monitoring profiles, etc.

OCR Server Requirements



You need to set up at least one OCR Database Node and one Mining Node for the OCR features to work.




No of Users*	Server Requirements	EC2 Instance Type
Less than 200 users	1 OCR Database Node	<ul style="list-style-type: none">m4.xlarge
	1 OCR Mining Node	<ul style="list-style-type: none">m4.4xlarge
Larger deployments of 200 or more users	1 OCR Database Node	<ul style="list-style-type: none">m4.xlargeDisk: 100 GB
	1 OCR Mining Node per 200 users	<ul style="list-style-type: none">m4.4xlargeDisk: 24 GB

*The requirements are applicable for a typical user who works on a single computer with Full HD (1920x1080) screen resolution, doing regular office work. If the users have multiple screens, higher-resolution screens, or have an unusual work pattern (e.g., watching many videos) then the requirements will be higher.



You will need to adjust the disk size as you add or remove video recordings over time. See the [Storage Requirements](#) section below for more information.

Storage Requirements

Primary Storage	<p>The Teramind virtual appliance comes with a primary volume of 50 GB by default. This volume contains the Teramind server application and database. The size of this volume can be increased at a later point in time.</p> <ul style="list-style-type: none"> Teramind requires the primary volume to be on SSD or equivalently fast storage for deployments above 500 users. BI Classifications needs about 5GB of disk space plus additional disk space equivalent to about 20% of your current DB size. So for example, if you have a database of 100GB the BI deployment will need 20GB+5GB = 25GB space. Check out this KB article to learn how to update your BI classifications.
Storage for Screen Recordings	<p>The simplest way to add scalable storage is to use AWS S3 Storage. For instruction on how to do so, check out this step.</p> <ul style="list-style-type: none"> S3 Storage is mandatory if you have a multi-server deployment (a deployment that has more than one Teramind App Server).

Agent Requirements

Supported Platforms	<ul style="list-style-type: none">• Microsoft Windows 8 and up (64-bit)• Microsoft Windows Server 2012 and up• macOS 13 (Sonoma), macOS 12 (Monterey), macOS 11 (Big Sur), macOS 10.15 (Catalina) and macOS 10.14 (Mojave) * <p><i>* At the moment, Teramind on Mac has limited functionalities. check out what features are currently supported here.</i></p>
Sessions	<ul style="list-style-type: none">• Stand-alone workstation / server• Terminal server (RDS) *• Application / Session server• Citrix• VMware Horizon <p><i>* Ideally, terminal servers should have a maximum of about 30 users or less depending on the number of screens and monitoring settings. Otherwise, you may have a performance impact.</i></p>
Load	Approximately 30 MB - 50 MB memory and 1-3% CPU utilization, depending on user activity
Visibility	Hidden or revealed desktop agents available
Deployment	<ul style="list-style-type: none">• Silent MSI• Deployment via Group Policy or SCCM• Dashboard-based silent remote installer
Bandwidth	Approximately 10 kbps upstream depending on user activity level & number of screens
Offline Storage	<p>Teramind features offline recording on the Silent/Hidden Agent (Windows). This means that in case of network downtime, the agent will save all data locally, and continue to enforce the policies and rules. Once the connection is re-established, the agent will upload the data to the server at a throttled pace.</p> <p>The offline storage buffer is configurable in monitoring settings and takes approximately 1GB per 160 hours of work time.</p>



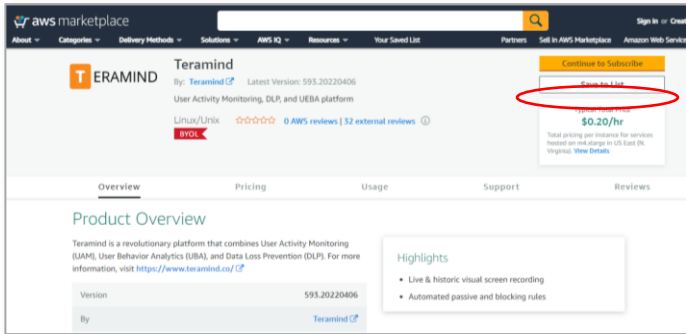
Detailed agent specifications can be found on our Knowledge Base [here](#).

Prerequisites

To get started, you will need:

- An AWS account
- Your Teramind license key, available from Teramind Self-Hosted portal at: <https://www.teramind.co/portal>
- An SSH client like Putty if you are using Windows

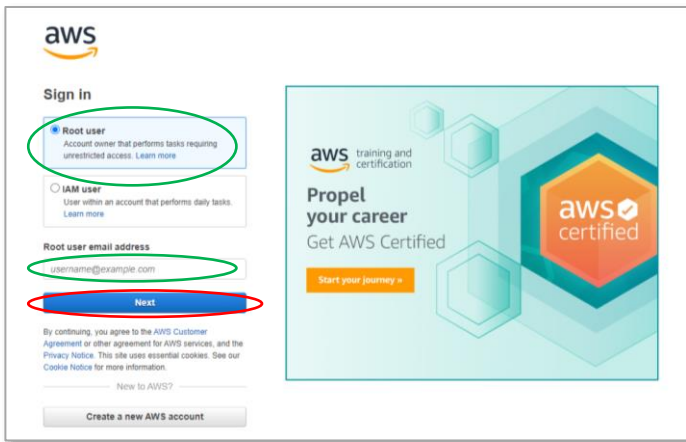
1 Creating an AWS Instance



Step 1-1

Visit: <https://www.teramind.co/deployment/aws> and click the **Check out Teramind on Amazon Marketplace** button, which will take you to the *Overview* tab on Teramind's deployment page on AWS.

Once there, click the **Continue to Subscribe** button on the top-right corner.



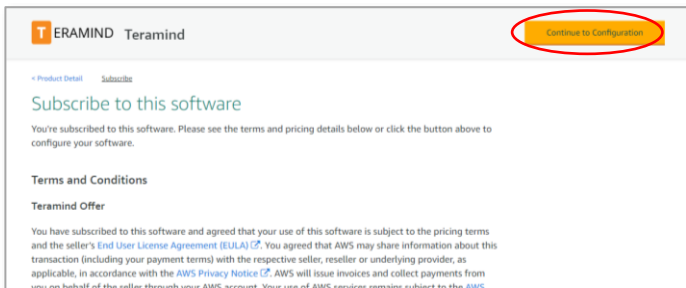
Step 1-2

If you are not signed in to your AWS account already, you will be asked to sign in.

Note that you will need a **Root user** account to be able to follow the steps on this guide.

Enter the **root user email address** and click the **Next** button.

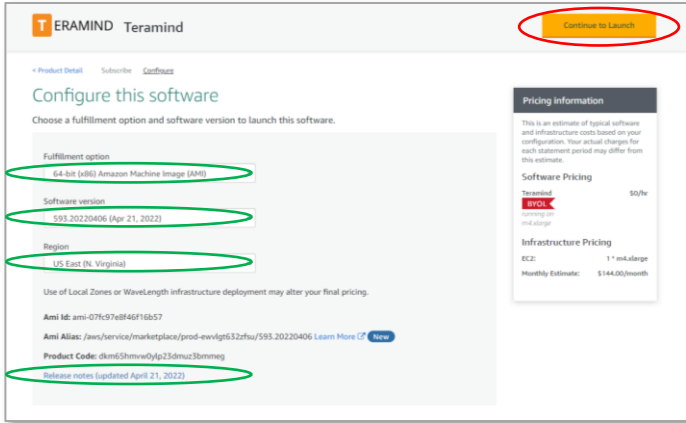
On the next screen, enter the password (and complete any CAPTCHA challenge) to sign in.



Step 1-3

On the *Subscribe* tab, you will be shown the Teramind terms and conditions and the offer effective data/expiration information.

Click the **Continue to Configuration** button on the top-right corner.



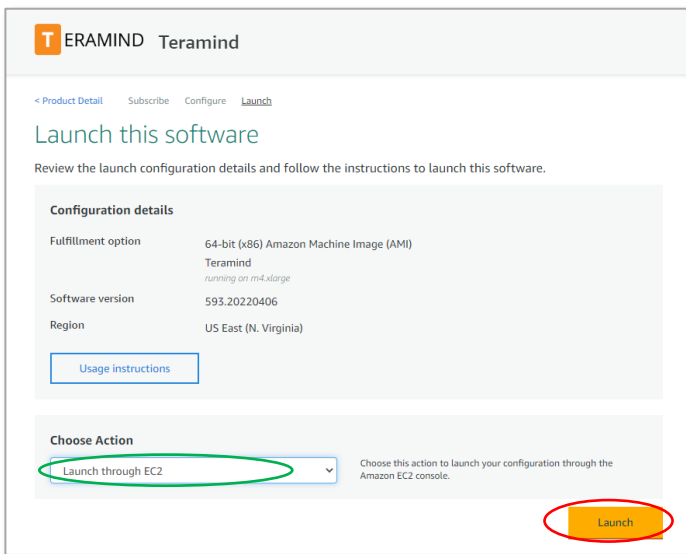
Step 1-4

On the *Configure* tab, you can choose the **Fulfillment Method**, **Software Version**, and the **Region**. Be sure to select a region closest to you for better performance.

You can click the **Release notes** link at the bottom to see the release notes for the selected Software Version.

On the right, you will see the pricing information.

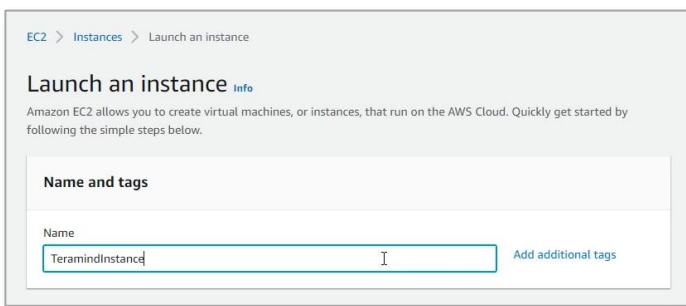
Click the **Continue to Launch** button when done.



Step 1-5

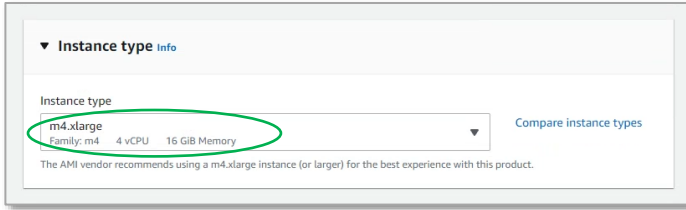
On the *Launch* tab, click the *Choose Action* pull-down menu and select **Launch through EC2** option.

Click the **Launch** button. This will take you to the *Launch an instance* screen.



Step 1-6

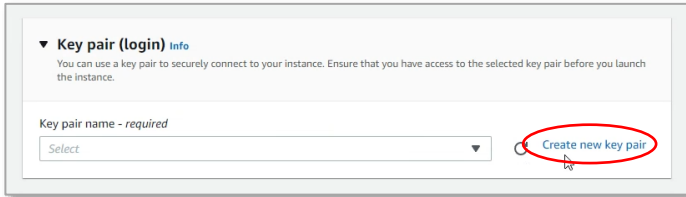
On the *Launch an instance* screen, under *Name and tags*, enter a name for your instance. For example, **TeramindInstance**.



Step 1-7

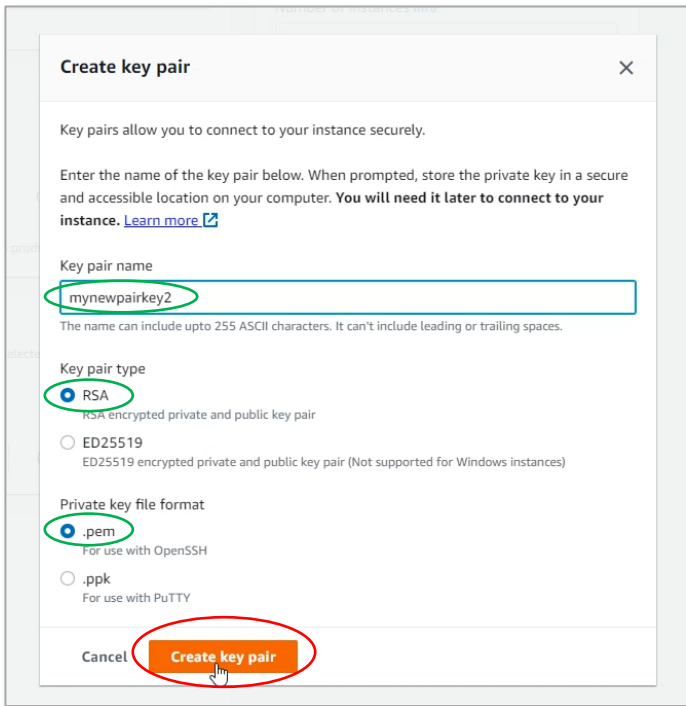
Select an instance under the *Instance type* section. For example, m4.xlarge with 4 vCPU and 16 GB memory.

For recommended instances, check out the [Primary Server Requirements](#) section on this guide.



Step 1-8

Click the **Create new key pair** link under the *Key pair (login)* section. This will pop up a *Create key pair* window.

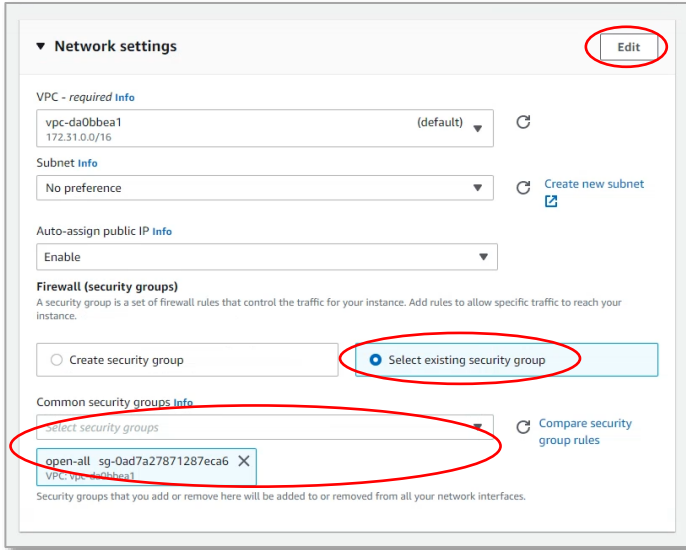


Step 1-9

On the *Create new key pair* pop-up window, Enter a name for the key pair. For example, **mynewpairkey2**.

Make sure **RSA** is selected under the *Key pair type* and **.pem** is selected for the *Private key file format*.

Click the **Create key pair** button then save the file in a secure location. You will need it in [Step 4](#) to connect to your instance.

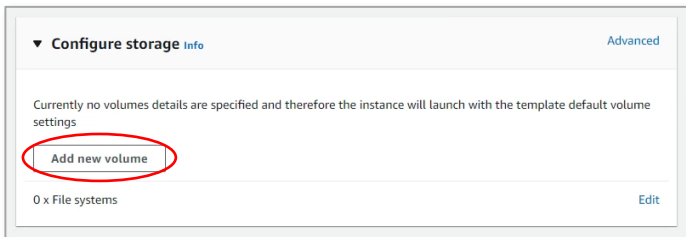


Step 1-10

Click the **Edit** button next to the Network settings section.

Then choose the **Select existing security group** option under *Firewall (security groups)*.

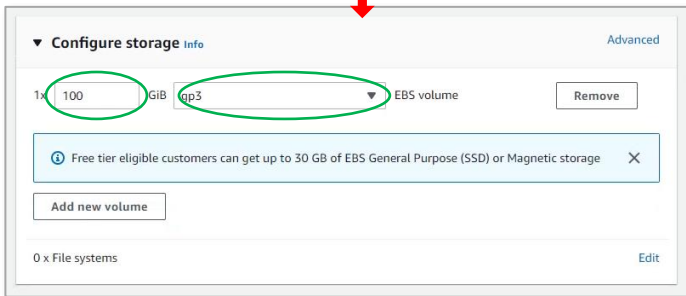
Finally, choose the **open-all** security group from the *Common security groups* list.



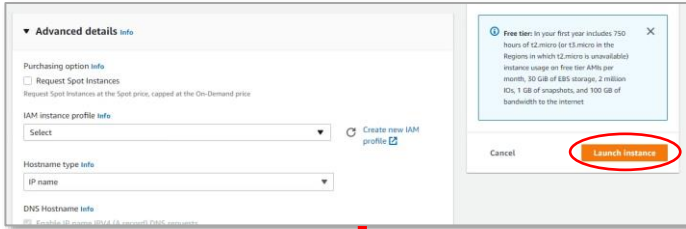
Step 1-11

Click the **Add new volume** button under the *Configure storage* section. This will add a new storage and let you enter options for it.

Enter a storage size in Giga Byte, for example **100** and select the type of volume, e.g., **gp3**.

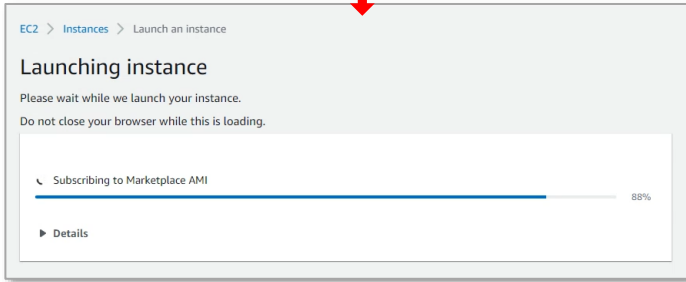


For recommended storage configurations, check out the [Storage Requirements](#) section on this guide.

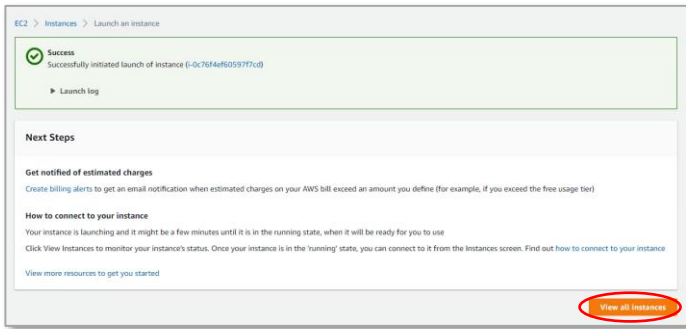


Step 1-12

If you want, you can configure *Advanced details* such as request a spot instance, change host name type, set auto-recovery option, etc. However, for this example, we do not need to change any of the advanced settings.

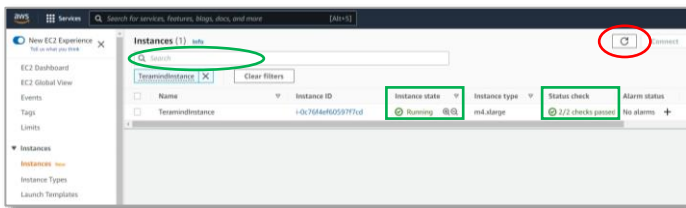


Click the **Launch instance** button. This will launch the instance and show a progress screen with the message, “*Subscribing to Marketplace AMI*”. Do not close your browser while the operation is taking place.



Step 1-13


Once the *Success* screen is shown, click the **View all instances** button. This will take you to a window with a list of your instances.



Step 1-14

On the *Instances* screen, you can enter your instance name in the **Search** box to narrow down the list.

Wait and pay attention to the **Instance state** and **Status check** columns. When the *Instance state* column says “*Running*” and the *Status check* column shows all the “*checks passed*”, it means your instance is ready for use.

Note: you can click the **Refresh**  button on the top to refresh the page and see the latest status.

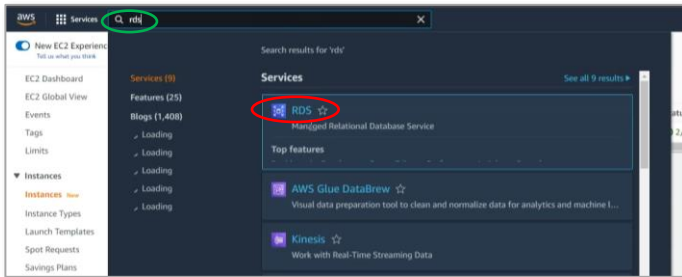


Keep this window open as you will need it in [Step 4](#).

2 Creating an RDS Database

External databases are not mandatory in Teramind. However, you may want to use them to improve the scalability of your platform. External databases are also highly recommended for deployments over 100 concurrent users.

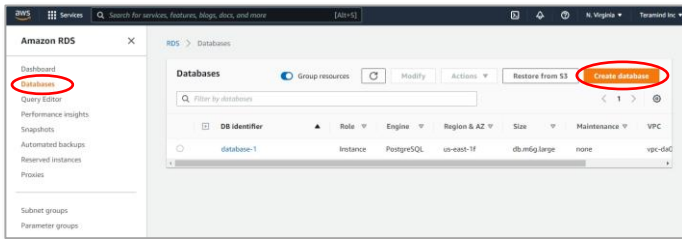
This section of the guide will show you how to create an AWS RDS database to be used with Teramind. If you already know how to do it, you can skip this section.



Step 2-1

From your *EC2 Management Console* page, on the top *Search* box, type **RDS**.

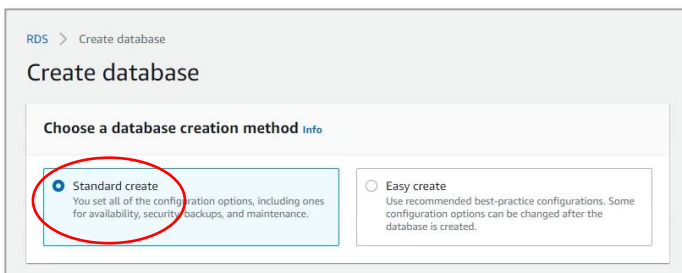
Select the **RDS** (Managed Relational Database Service) from the list of services. You will be taken to the *RDS Management Console* page.



Step 2-2

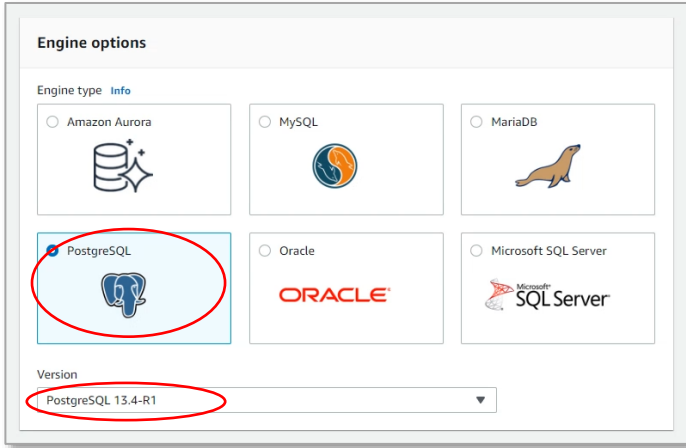
On the *RDS Management Console* page, select **Databases** from the left-hand sidebar.

Then, click the **Create database** button on the top-right corner of the screen.



Step 2-3

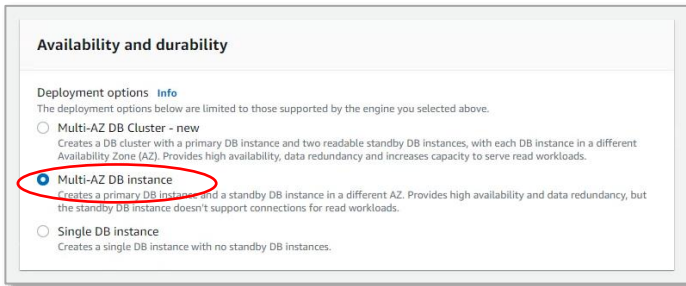
On the *Create database* screen, select **Standard create** under the *Choose a database creation method*.



Step 2-4

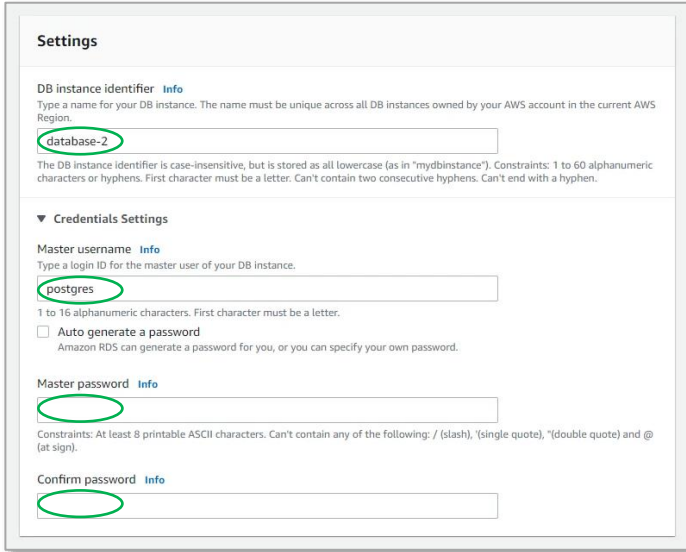
Select **PostgreSQL** under the *Engine options* section.

Select the latest *Version* for the database. For example, **PostgreSQL 13.4-R1**.



Step 2-5

Under the *Availability and durability* section, select the **Multi-AZ DB instance** option.



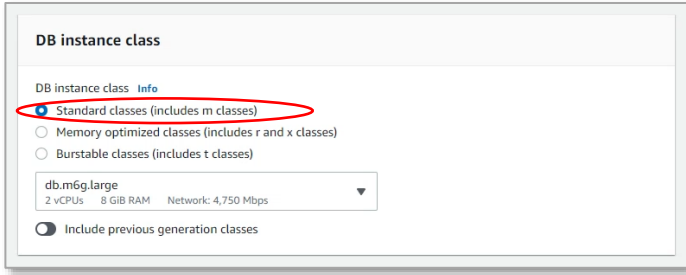
Step 2-6

Under the *Settings* section, type a name in the *DB instance identifier* field. For example, **database-2**. Assign a *Master user name* such as **postgres**.

Enter a **Master password** and confirm it.

Remember or take note of the username and password as you will need them in [Step 4](#).

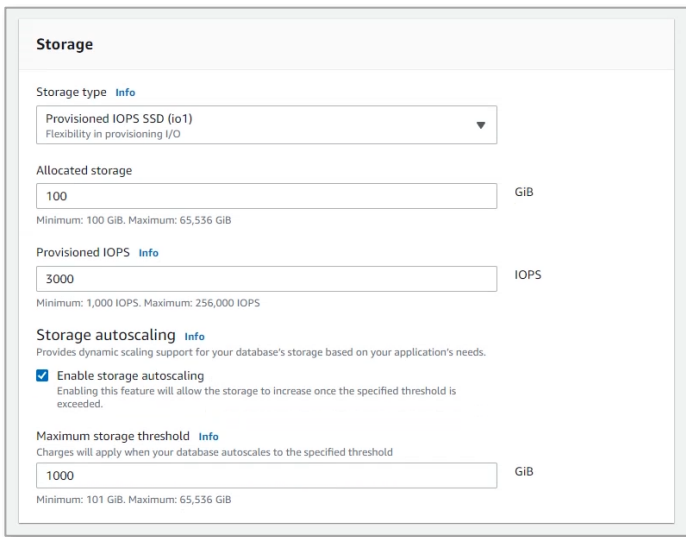
Scroll down until you reach the *DB instance class* section.



Step 2-7

Under the *DB instance class* section, select the **Standard classes** option.

For recommended DB instances, check out the [Database Server Requirements](#) section on this guide.



Step 2-8

For this example's purposes, you can keep the default settings as is under the *Storage* section.

For recommended storage configurations, check out the [Database Server Requirements](#) section and for general storage guidelines, check out the [Storage Requirements](#) section on this guide.

Connectivity

Virtual private cloud (VPC) Info
VPC that defines the virtual networking environment for this DB instance.
Default VPC (vpc-da0bbea1) ▼
Only VPCs with a corresponding DB subnet group are listed.

After a database is created, you can't change its VPC.

Subnet group Info
DB subnet group that defines which subnets and IP ranges the DB instance can use in the VPC you selected.
default ▼

Public access Info
 Yes
Amazon EC2 instances and devices outside the VPC can connect to your database. Choose one or more VPC security groups that specify which EC2 instances and devices inside the VPC can connect to the database.
 No
RDS will not assign a public IP address to the database. Only Amazon EC2 instances and devices inside the VPC can connect to your database.

VPC security group
Choose a VPC security group to allow access to your database. Ensure that the security group rules allow the appropriate incoming traffic.
 Choose existing
Choose existing VPC security groups Create new
Create new VPC security group

Existing VPC security groups
Choose VPC security groups
default × open-all ×

▶ Additional configuration

Step 2-9

Under the *Connectivity* section, you can configure various connectivity options according to your needs.

For this tutorial's purposes we will use the following settings:

Select **Default VPC** for the *Virtual private cloud (VPC)* option.

Select **Yes** for the *Public access* option.

Select **Choose existing** for the *VPC security group* option.

Under the *Existing VPC security groups*, select the **default** and **open-all** options.

Database authentication

Database authentication options Info
 Password authentication
Authenticates using database passwords.
 Password and IAM database authentication
Authenticates using the database password and user credentials through AWS IAM users and roles.
 Password and Kerberos authentication
Choose a directory in which you want to allow authorized users to authenticate with this DB instance using Kerberos Authentication.

▶ Additional configuration
Database options, encryption enabled, backup enabled, backtrack disabled, Performance Insights enabled, Enhanced Monitoring enabled, maintenance, CloudWatch Logs, delete protection enabled.

You are responsible for ensuring that you have all of the necessary rights for any third-party products or services that you use with AWS services.

Cancel **Create database**

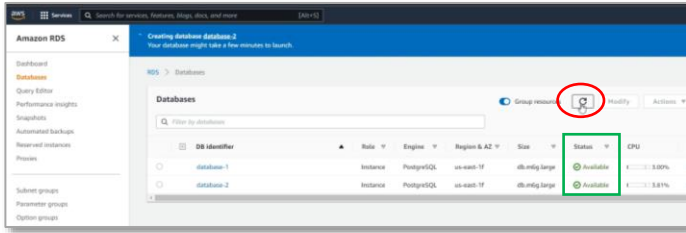
Step 2-10

Under the *Database authentication* section, select **Password authentication** for the *Database authentication options*.

Under the *Additional configurations* section, you can specify additional options such as encryption, backup, enhanced monitoring, etc. For this tutorial's purposes, we will keep them to their default settings.


Under the *Estimated monthly costs* section, you will be able to see the cost breakdown for your database.


Once ready, click the **Create database** button at the bottom to create the database. It might take a few minutes for the database to be ready.



Step 2-11

On the *Databases* screen, wait and pay attention to the **Status** column. When the *Status* column says, “Available”, it means your database is ready for use.

Note: you can click the **Refresh**  button on the top to refresh the page and see the latest status.

 Keep this window open as you will need it in [Step 4](#).

3 Adding an S3 Storage

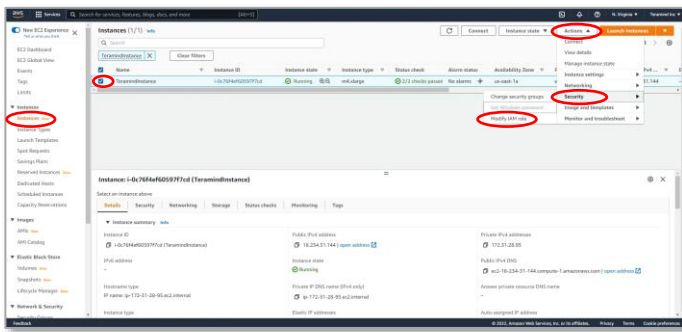
Teramind does not need external storage. However, Teramind can utilize a file storage system for screen and audio recordings, captured attachments, printer documents, and metadata such as user images. AWS S3 is an efficient, secure, scalable, and redundant solution to store objects like these. The S3 storage will improve the scalability of your platform and is recommended for deployments of over 100 concurrent monitored users.



For more information, check out the [Storage Requirements](#) section of this guide.

To use the AWS S3 storage, you will need to attach an Identity and Access Management or IAM profile to your storage instance. IAM enables you to manage access to your AWS services and resources securely. Using IAM, you can create and manage AWS users and groups and control user permissions.

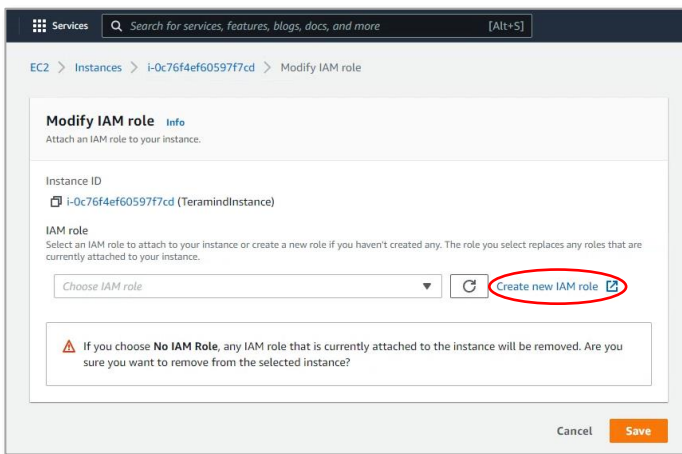
This guide will show you how to create an IAM profile and attach it to your S3 instance. If you already know how to create one, you can skip this section.



Step 3-1

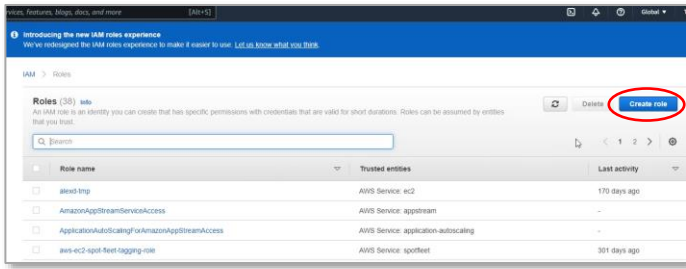
Go to the **Instances** screen from your *EC2 Management Console*. Make sure the instance you want to use is selected.

Click the **Actions** button near the top-right corner. From the pull-down menu, select **Security > Modify IAM role**.



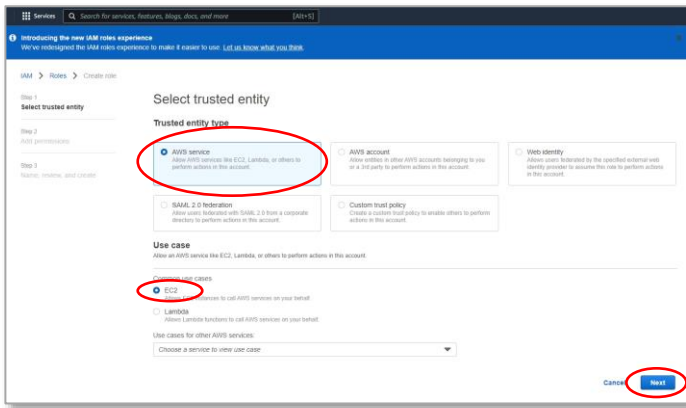
Step 3-2

On the *Modify IAM role* screen, click the **Create new IAM role** link.



Step 3-3

On the *Roles* screen, click the **Create role** button.

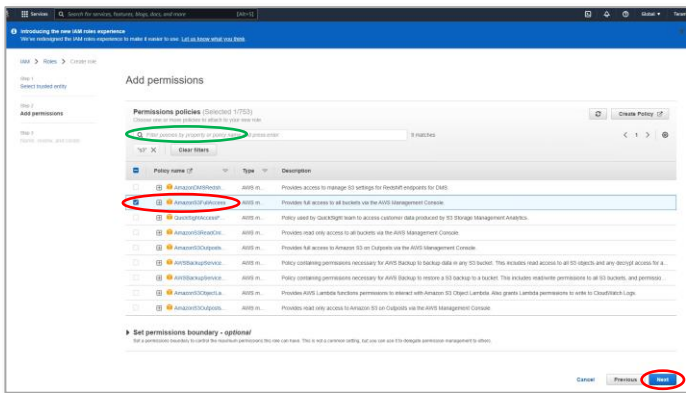


Step 3-4

Select the default **AWS service** option under the *Trusted entity type* section.

Select the **EC2** option under *Use case* section.

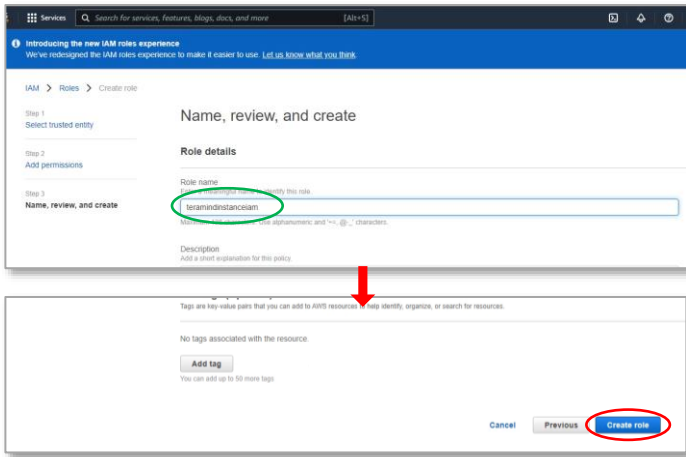
Click the **Next** button to continue.



Step 3-5

From the list of permission policies, select the one named '**AmazonS3FullAccess**' (you can type in the **Search** field to quickly locate it from the list of permission policies).

Click the **Next** button to continue.

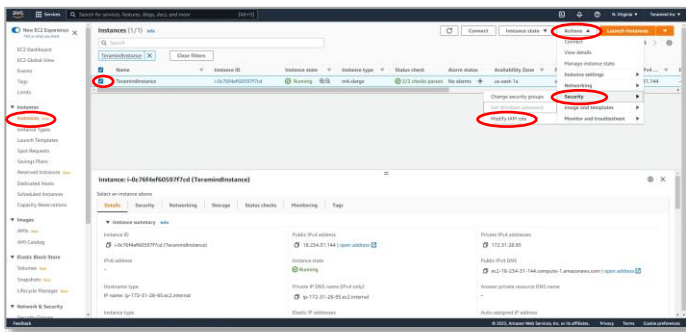


Step 3-6

Under the *Role details* section, enter a *Role name*, e.g., **teramindinstanceiam**.

On this screen, you can also add a description for the role, select trusted entities, add tags, etc. But for this example, we will not need any of those.

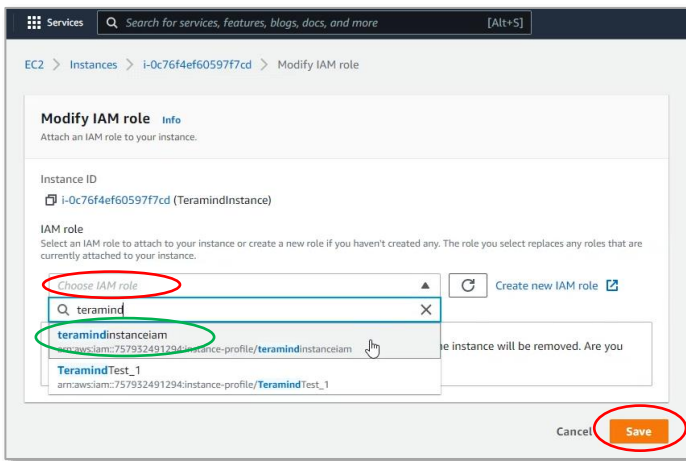
Scroll down to the bottom and click the **Create role** button.



Step 3-7

Go back to the **Instances** screen from your *EC2 Management Console*. Make sure the instance you want to use is selected.

Click the **Actions** button near the top-right corner. From the pull-down menu, select **Security > Modify IAM role**.



Step 3-8

On the *Modify IAM Role* screen, click the **Choose IAM role** field and type or select the IAM role you created in the previous steps (**teramindinstanceiam**).

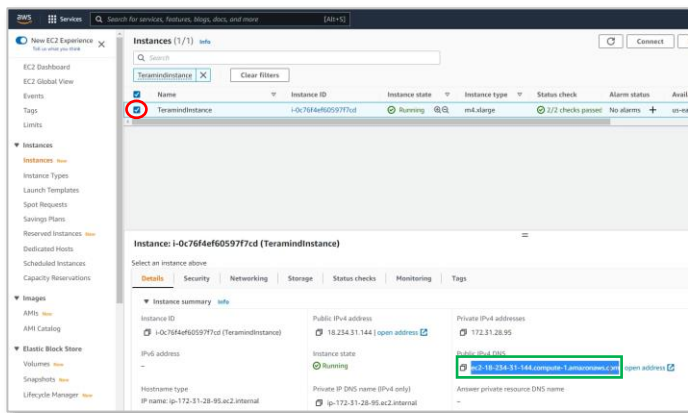
Click the **Save** button to attach the IAM role to your instance.

4 Finishing the Deployment

As the last step of the server deployment process, you will need to assign the external database and storage to your master instance, setup the Teramind Server using the SSH and finally, configure your account settings on the Teramind Dashboard.



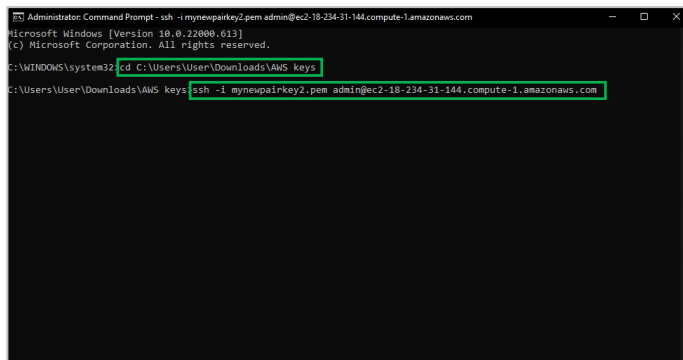
After you finish the deployment, you should update your server and apply any latest patch. Check out this article on our Knowledge Base: [How to update the Teramind Server and BI Classification \(On-Premise / Private Cloud deployment\)](#).



Step 4-1

Go back to the *Instances* window you left open in [Step 1-14](#).

Select the master instance you created (e.g., **TeramindInstance**). Copy or write down the **Public IPv4 DNS** address for the instance you created (e.g., **ec2-18-234-31-144.compute-1.amazonaws.com**).



Step 4-2

Launch an SSH session. If you are on Windows, you can use a tool like Putty or a similar utility for the SSH. Make sure you have administrative access.

Change to the folder/directory where you downloaded the key pair file in [Step 1-9](#) by using the CD command. For example,
`cd
c:\Users\User\Downloads\AWS keys`

Type:
`ssh -i <pem file> admin@<DNS>`

Where *<pem file>* is name of the key pair file you downloaded in [Step 1-9](#) (e.g., *mynewpairkey2*).

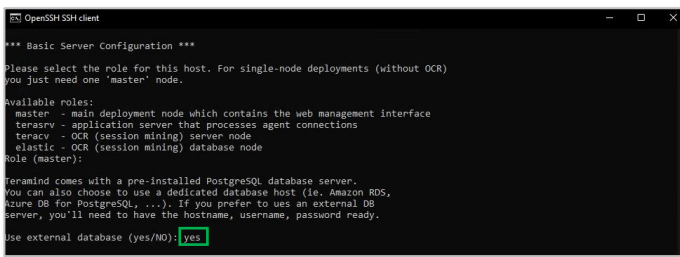
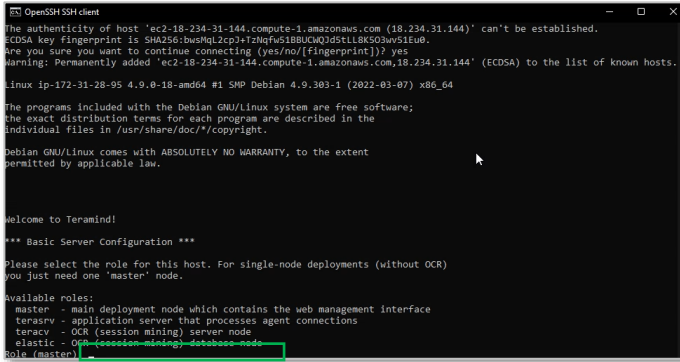
<DNS> is the Public IPv4 DNS address you copied in the previous step (e.g., `ec2-18-234-31-144.compute-1.amazonaws.com`).

Press **Enter**.

Step 4-3

Once the server is ready, you will see this message, 'Welcome to Teramind!'. Under the message you will be given options to assign roles for the nodes/hosts, beginning with the Master role.

Enter a **name** at the *Role (master)* prompt or just press **Enter** to keep the default name.



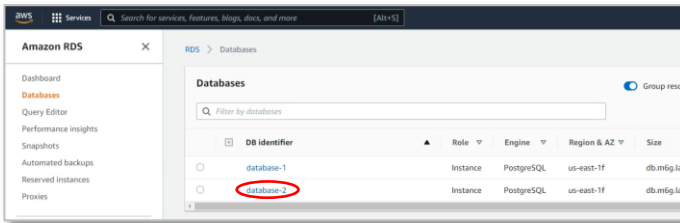
Step 4-4

At the *Use external database (yes/NO)* type **yes** and press **Enter**.

Step 4-5

Go back to the *Databases* window you left open in [Step 2-11](#).

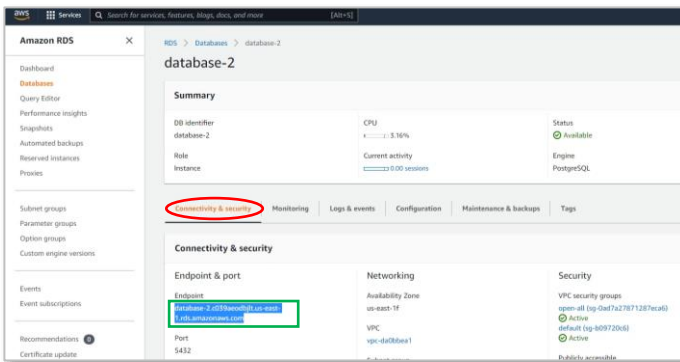
Click the name of the database you created (e.g., `database-2`). This will take you to the selected database's page.



Step 4-6

On the database's page, click the **Connectivity & security** tab.

Copy the **hostname** under Endpoint (e.g., `database-2-c039aeodbj1t.us-east-1.rds.amazonaws.com`)




```
OpenSSH SSH client
*** NOTE ***
Teramind requires two databases named 'teramind' and 'te_on-site'.
If those databases do not exist, the installation process will
attempt to create them. Therefore, CREATEDB permissions are
necessary.
***

Database IP or hostname: database-2.c899ae0bj1t.us-east-1.rds.amazonaws.com
Database username: postgres
Database password: _____
```

Step 4-7

Go back to the SSH windows.

When prompted, paste the **Database IP or hostname** you copied in the previous step.

At the following prompts, enter the **Database username** and **Database password** you created in [Step 2-6](#).

```
admin@ip-172-31-28-96 ~
ALTER TABLE
Done
Updating database config...

Teramind can store screen recordings and other non-meta-data as flat files or
as objects in a S3-compatible bucket.

Use S3 for storing data (yes/NO): yes

*** NOTE ***
This host should have IAM role for accessing S3.
***

Teramind can use existing S3 buckets or create new ones.

Create new buckets (yes/no): yes
Enter bucket name for screen recordings: teramindinstancebucket1
Enter bucket name for user content (ie. attachments, printed documents, ...): teramindinstancebucket2
Enter bucket name for Teramind application objects: teramindinstancebucket3
Created symlink /etc/systemd/system/multi-user.target.wants/teramind.service -> /etc/systemd/system/teramind.service.

Teramind initial configuration is complete. Please open https://18.234.31.144/ in
a browser to continue system setup.

admin@ip-172-31-28-96:~$
```

Step 4-8

After Teramind has finished the database initializations, it will show the prompt, *Use S3 for storing data?*. Enter **Yes**.

Enter **Yes** at the *Create new buckets?* prompt.

Then you will be prompted to enter names for three buckets: one for screen recordings, one for user content i.e. attachments or printer docs, and the third one for application objects. Give unique names to each bucket (e.g., **teramindinstancebucket1**, **teramindinstancebucket2**, and **teramindinstancebucket3**).

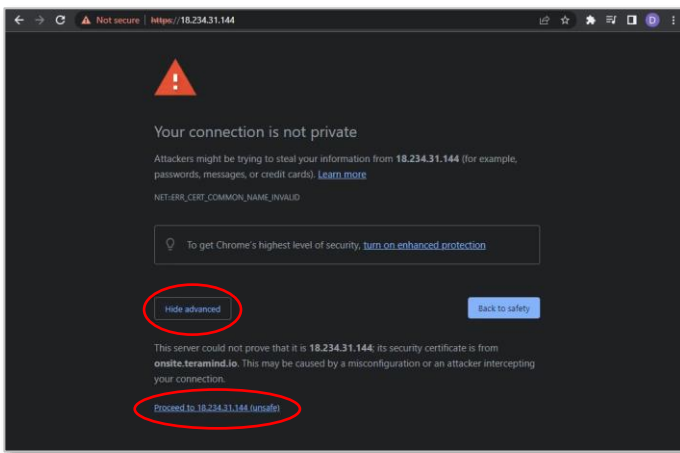
*Please see the **S3 Bucket Naming Requirements** below for information on rules related to the naming of the buckets.*

Once you have entered the bucket Teramind will set up the servers. Finally, you will be provided with a **link** to your dashboard (e.g., **https://18.234.31.144/**). Click the link or enter it on your browser to continue.

S3 Bucket Naming Requirements

The S3 buckets must have a name that conforms with the naming requirements for non-US Standard regions. Amazon S3 defines a bucket name as a series of one or more labels, separated by periods, that must adhere to the following rules:

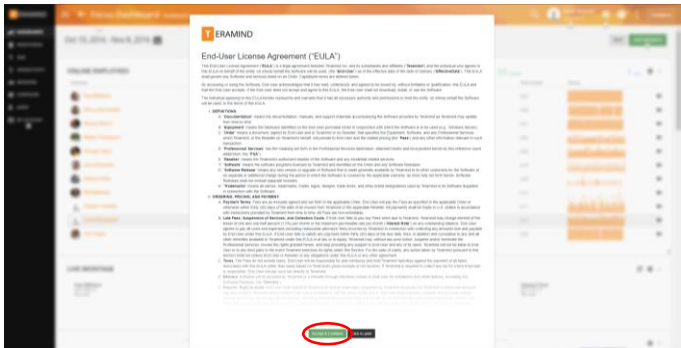
- The bucket name can be between 3 and 63 characters long and can contain only lower-case characters, numbers, periods, and dashes.
- Each label in the bucket name must start with a lowercase letter or number.
- The bucket name cannot contain underscores, end with a dash, have consecutive periods, or use dashes adjacent to periods.
- The bucket name cannot be formatted as an IP address, i.e. 198.51.100.24.



Step 4-9

When you open the Teramind Server link in the browser, you may be displayed a warning message. This is because you are using an HTTPS connection without an SSL certificate. Most browsers will allow you to continue with an override action.

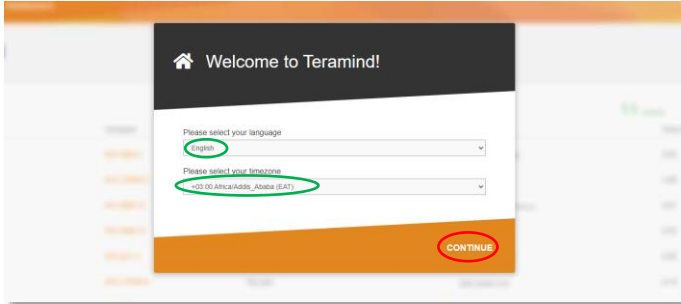
If you are using Google Chrome, click the **ADVANCED** link on the page and select the **Proceed to...** option.



Step 4-10

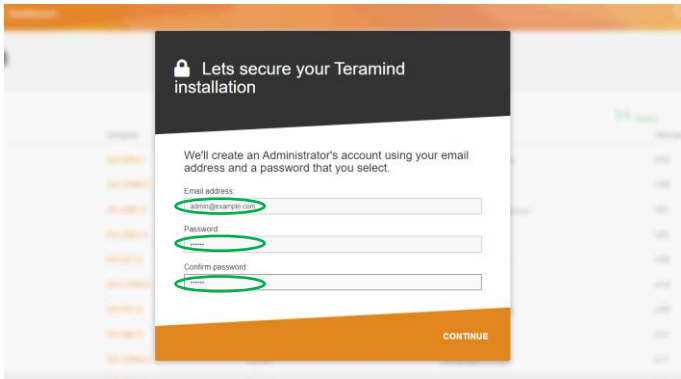
When you enter the Teramind Dashboard for the first time, you will see the *End-User License Agreement* screen.

Scroll down and click the **Accept & Continue** button.



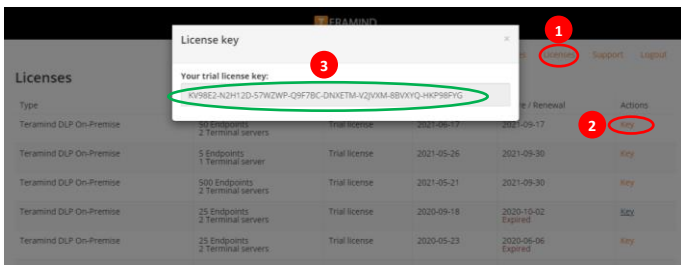
Step 4-11

On the *Welcome to Teramind* screen, select your **language** and **timezone** and click **CONTINUE**.



Step 4-12

On the *Let's secure your Teramind installation* screen, enter an **email** and a **password** for your Admin account.



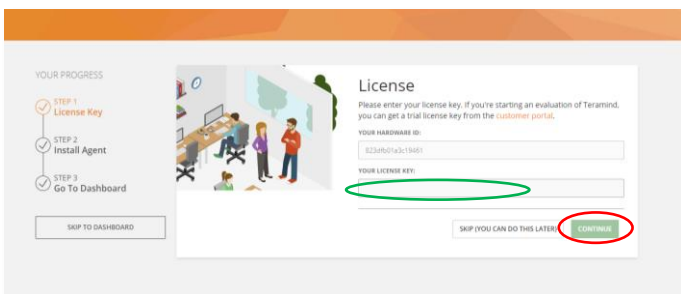
Step 4-13

Open a new browser tab and go to: <https://www.teramind.co/portal>. Login with the admin email and password.

Click the **Licenses** tab.

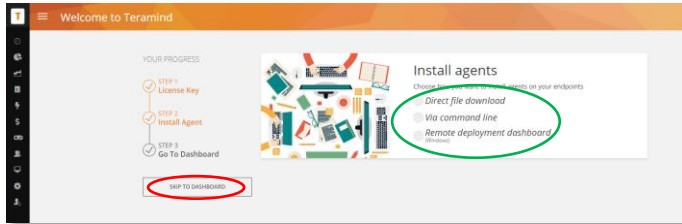
From the list of licenses, click the **Key** link under the *Actions* column. A pop-up will display the license key.

Copy the **license key** or write it down.



Step 4-14

Go back to your Teramind Dashboard. Enter the **license key** and click the **CONTINUE** button.



Step 4-15

At this stage, you can install the Teramind agent and start monitoring the targeted computer(s). Or, you can do it later.

To install the agent, click one of the [options](#) under *Install agents*. If you need help installing the agent, check out [this article](#) on our Knowledge Base. You can also watch this short video: [Downloading and Installing Teramind's Hidden Agent](#)

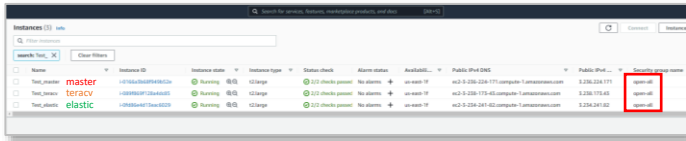
To install the agent at a later time, click the **SKIP TO DASHBOARD** button.



You are done setting up your Teramind Server. If you want to use the OCR feature, continue to the [Step 5](#) below.

5 Setting up the OCR (optional)

If you want to use the OCR feature, you will need to set up two nodes in addition to a master node.



Step 5-1

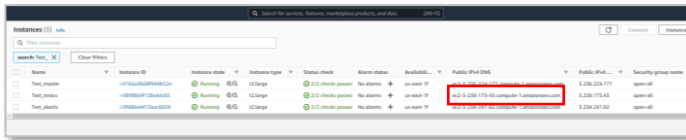
Create the *master* VM as usual.

Then, create two additional VMs. The first node will store the OCR videos. In Teramind, we will refer to it as *teracy*. The second node is for the OCR database. In Teramind, we will refer to it as *elastic*.

Make sure all the nodes are in the same **Security Group**.

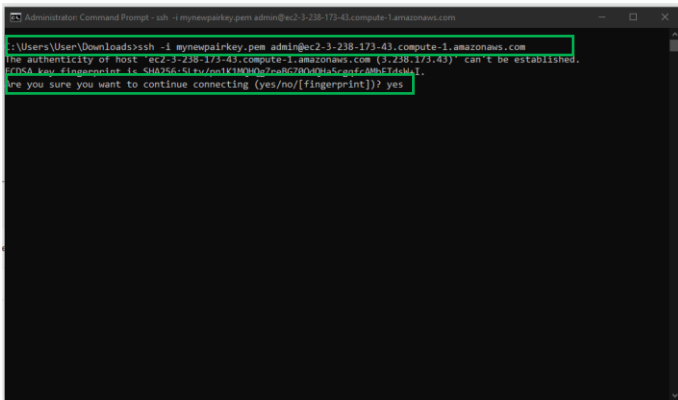


For more information on the OCR server requirements, check out the [OCR Server Requirements](#) section on this guide.



Step 5-2

From your AWS portal's *Instances* page, copy the **Public IPv4 DNS** address for the *teracy* instance.



Step 5-3

Launch an SSH session. If you are on Windows, you can use a tool like Putty or a similar utility for the SSH. Make sure you have administrative access.

Type:
`ssh -i "<pem file>"
admin@<DNS>`

Where *<pem file>* is the full path of the key pair file you downloaded when creating the *teracy* VM.

<DNS> is the Public IPv4 DNS you copied in the previous step (Step 5-2).

If prompted to confirm the connection, enter **yes**.

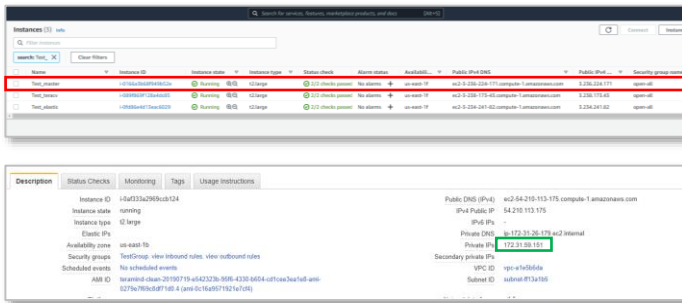
Press **Enter**. The server will be ready in a few minutes.

Step 5-4

On the AWS portal's *Instances* page, select the **master** instance.

At the bottom of the screen, you will notice a *Description* panel is shown.

Copy or write down the **Private IP** address from the *Description* panel.



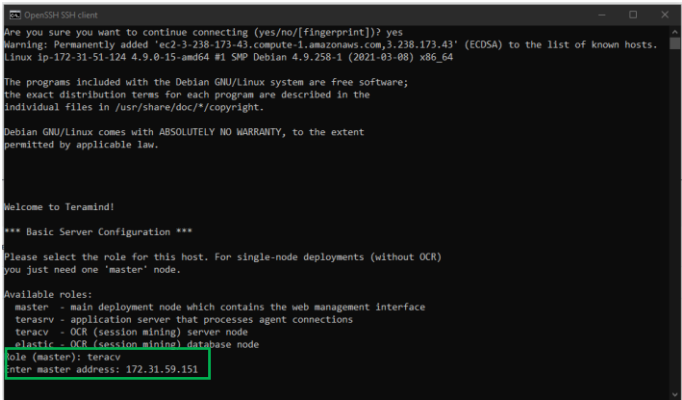
Step 5-5

Go back to the command prompt window.

When asked, enter **teracv** at the *Role (Master)* prompt.

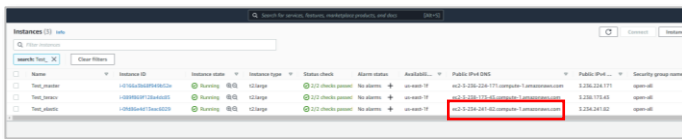
Paste the **Private IP address** you copied in the previous step (Step 5-3).

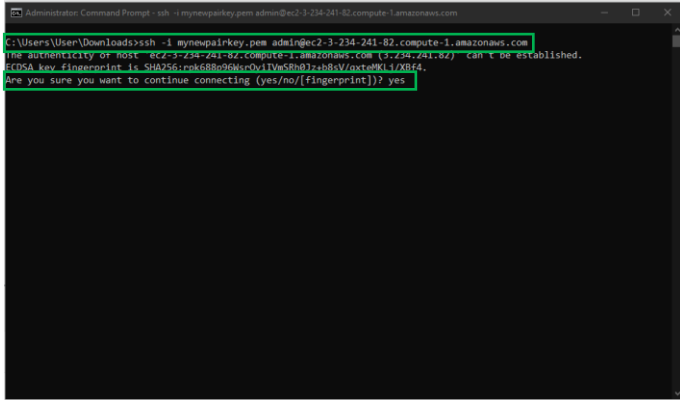
It will take a few minutes for Teramind to set up the *teracv* node.



Step 5-6

From your AWS portal's *Instances* page, copy the **Public IPv4 DNS** address for the *elastic* instance.





Step 5-7

Launch an SSH session. If you are on Windows, you can use a tool like PuTTY or a similar utility for the SSH. Make sure you have administrative access.

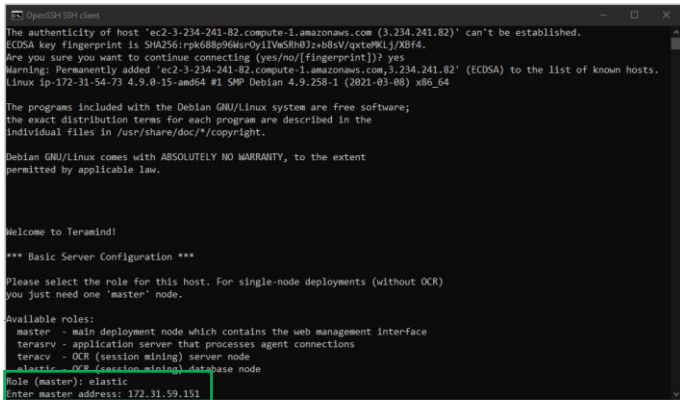
Type:
`ssh -i "<pem file>"
 admin@<DNS>`

Where *<pem file>* is the full path of the key pair file you downloaded when creating the *elastic* VM.

<DNS> is the Public IPv4 DNS address you copied in the previous step (Step 5-6).

If prompted to confirm the connection, enter *yes*.

Press **Enter**. The server will be ready in a few minutes.

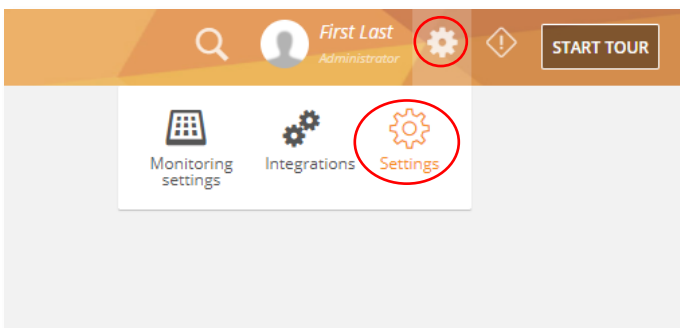


Step 5-8

When asked, enter *elastic* at the *Role (Master)* prompt.

Paste the *Private IP address* of the *master* node you copied in Step 5-4.

It will take a few minutes for Teramind to set up the *elastic* node.

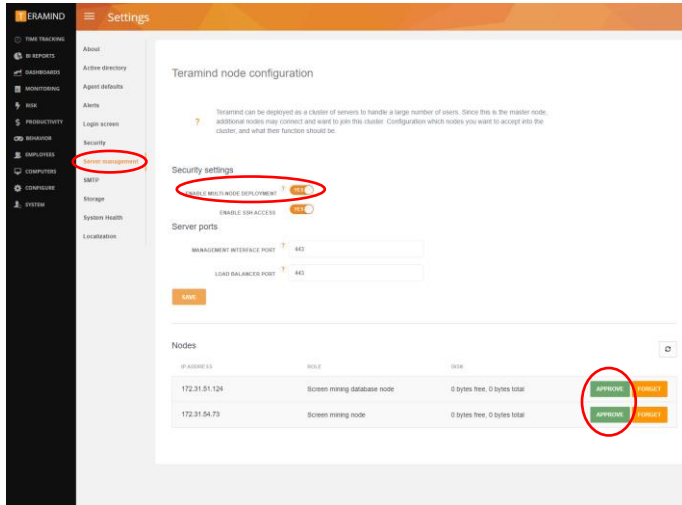


Step 5-9

We will now need to approve the two nodes on the Teramind Dashboard.

Login to your Teramind Dashboard on the master server.

Click the **Cog Wheel** icon near the top-right corner of the dashboard and select **Settings** from the pull-down menu.



Step 5-10

From the *Settings* screen, click the **Server management** tab.

Turn on the **ENABLE MULTI-NODE DEPLOYMENT** option under the *Security settings* section.

Under the *Nodes* section, you will notice the *Screen mining database node* and the *Screen mining node*.

Approve both nodes by clicking the **APPROVE** buttons.

You are now all setup for the OCR.

6 Installing the Teramind Agent

Teramind Agent can be installed both locally and remotely. Check out this article to learn how to download and install the agent: [How to download and install the Teramind Agent](#).

Firewall & Proxy Considerations

In most cases, you should not have to change any settings to get Teramind to work. By default, the Teramind Agents communicate with the Teramind server on two ports: 443, and 10000.

The Teramind management interface is entirely web-driven and runs over HTTPS (port 443). This means that most proxies will allow the traffic through, provided you properly installed your SSL certificates.

For live and recorded screen playback, as well as live session listing, Teramind uses Websockets. Although Websockets operates as HTTPS over port 443, some older proxies may not recognize this protocol. In either case, if you are experiencing trouble accessing your Teramind dashboard, try to disable your proxy temporarily to isolate the cause.

Also note that, if the audio recording is enabled, Teramind Agent will connect to the server on a random UDP port in the range 1000-65535 to send the audio recordings. Make sure UDP ports in that range are enabled and open from the endpoint to the server.



If you encounter any issues with your firewall or proxy, check out this troubleshooting article for help: [Firewall and proxy issues](#).

Antivirus Considerations

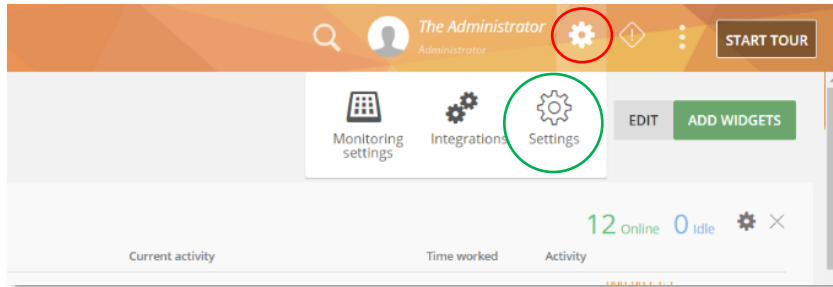
Teramind Agent and its drivers come digitally signed with an extended validation certificate. We've made every effort to coordinate our signature with the major antivirus vendors, and as a result, Teramind should work normally with the vast majority of antivirus software.




If you encounter any issues, check out the [Antivirus Configuration Guide](#) for help.

Additional Configurations

Once you have installed Teramind successfully, you can configure other aspects of the server, agent and other settings entirely from the web-based dashboard.



Once you have installed To access the configuration settings, hover over the **Cog icon**  on the top-right corner of the dashboard, and click **Settings**.

The *Settings* screen will open.

Here are a few key settings you should configure. For additional information, check out the [Settings](#) section on the Teramind User Guide.

Changing the License Key

If for any reason, you want to change the license key (for example, when upgrading from a trial to a paid account), you can do that from the **Settings > About** tab.

Check out this article for help: [How to change the license key \(On-Premise / Private Cloud Deployment\)](#).

Updating the Server

Teramind regularly releases server updates for the On-Premise deployment on our Self-Hosted Portal and the virtual machine images may not always contain the latest server updates. These updates may contain bug fixes, security patches and new features. To keep your deployment up-to-date, we recommend that you update your server regularly. To update your server, download the latest server image from the Self-Hosted Portal at www.teramind.co/portal. Under the Download > Teramind Update section. Download the platform update file (with a TMU extension) by clicking the download icon.

Once you have downloaded the file, you can upload it to the dashboard under Settings > About tab.

Check out this article for help: [How to update the Teramind Server and BI Classification \(On-Premise deployment\)](#).

Setting Up the Active Directory / LDAP Integration

Though not mandatory, Teramind can be integrated with Active Directory to import your users, computers, groups, attributes and other important meta-data. The LDAP attributes can then be used to create user/computer accounts and filter BI Reports.

You can configure Active Directory from the **Settings > Active Directory** tab.

Check out the [Settings > Active Directory](#) section on the Teramind User Guide to learn how to setup an Active Directory / LDAP integration.

SMTP Email

Configuring the SMTP settings is necessary for the Teramind server to be able to send outbound emails such as the daily digest emails sent to administrators, scheduled reports, low storage notifications, license alerts, and password recovery emails.

You can configure the SMTP from the Settings > SMTP tab.

Check out this article for help: [SMTP Configurations \(On-Premise\)](#).

SSL Certificate

Teramind strongly recommends proper configuration of SSL in order to avoid browser warnings and restrictions. Some browsers will not allow WebSocket communications if the certificates are invalid. This may prevent you from watching live screens or screen recordings.

Configuring the SMTP settings is also necessary for the Teramind server to be able to send outbound emails such as the daily digest emails sent to administrators, scheduled reports, low storage notifications, license alerts, and password recovery emails.

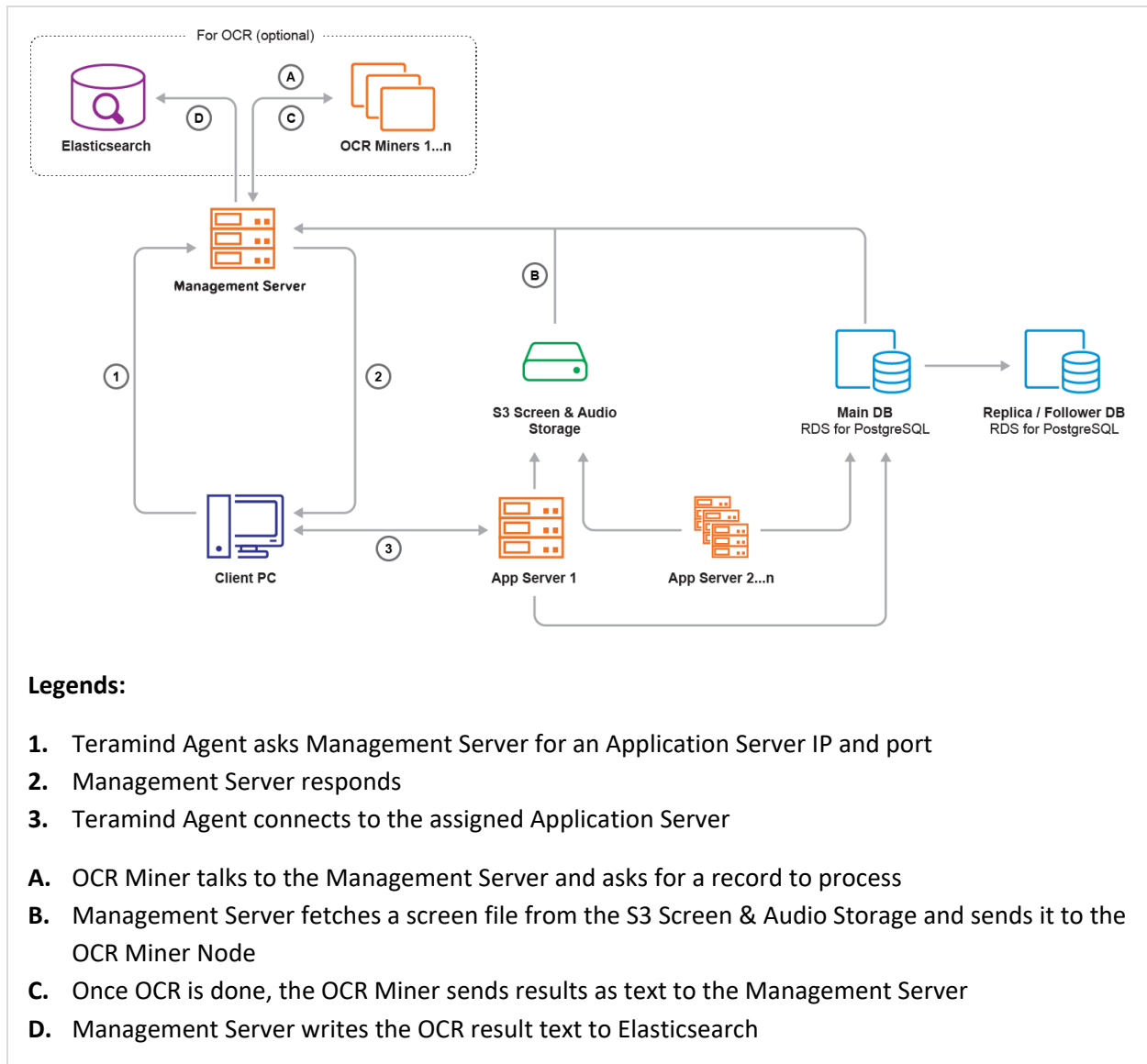
You can upload your SSL certificate from the Settings > SSL tab.

Check out the [Settings > SSL](#) section on the Teramind User Guide for more information. You can also create your own SSL certificates for use with your on-premise deployments.

To learn how to generate such self-signed certificates, check out [this article](#).

To learn how to use a third-party certificate, check out [this article](#).

Architecture



The **Management Server** serves the admin dashboard, load balances agents, and provides data to the OCR Miner Nodes. Teramind Agent connects to an **Application Server** via an always-on, TLS-encrypted connection, using our own protocol based on Google Protocol Buffers. **OCR Miners** are stateless and work with spot instances.

Technical Specifications

Regions / Data Centers	<p>Teramind on AWS is available on the following data centers/regions (subject to change). We recommend you choose a region closest to you for faster service and lower latency:</p> <ul style="list-style-type: none">• US East (N. Virginia)• US East (Ohio)• US West (N. California)• US West (Oregon)• Canada (Central)• EU (Frankfurt)• EU (Ireland)• EU (London)• EU (Paris)• Asia Pacific (Singapore)• Asia Pacific (Sydney)• Asia Pacific (Seoul)• Asia Pacific (Tokyo)• Asia Pacific (Mumbai)• South America (São Paulo)
OS	64-bit Linux/Unix, Debian 12 AMI.
Databases	EBS volume by default. Optionally S3, RDS/Postgres can be used as screen/audio recording storage.
Instances	Teramind supports various EC2 instances types (m4, t2, t3, m3, etc.) for different sizes (micro, large, extra large, etc.). Please check out the Primary Server Requirements section for more information.
License	BYOL (bring your own Teramind license). Click here to try or subscribe to Teramind on-prem/private cloud.

Installation Support and Troubleshooting

Chat	From your Teramind Dashboard or our website: https://teramind.co/
Email	support@teramind.co