Teramind On-premise v2 Deployment & Configuration Guide

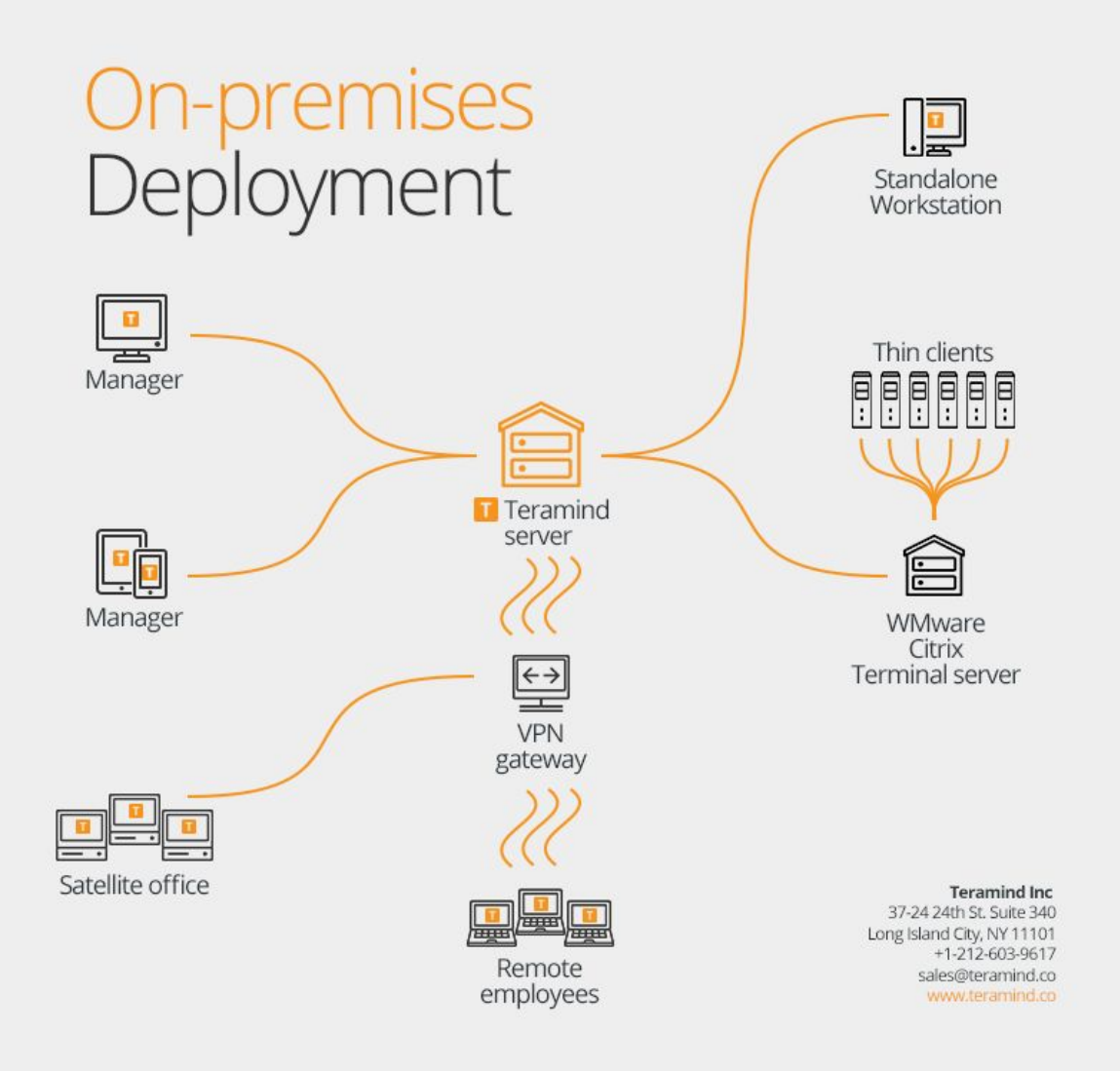
(single master-node deployment)

Overview

Teramind Enterprise is the world's leading platform for insider risk management, employee monitoring, and productivity analysis / workforce optimization. The platform is equally powerful as it is easy to deploy and configure. This guide outlines everything you need to set up Teramind in your organization, step-by-step.

Architecture

A single-server Teramind deployment uses a client – server architecture as outlined below.



For portability, simplification, and to better leverage your distributed hardware, Teramind comes only in the form of a virtual appliance. In its default configuration, the database is embedded into the virtual appliance, and therefore no external database is required.

System & Network Requirements

Required assets

In order to successfully deploy Teramind, you should have the following assets available on-hand. These assets are available from the download page of the customer portal.

- This document
- Teramind Server virtual machine image for your virtualization platform
- Teramind Agent: 32 and/or 64-bit (optional)
- Teramind Enterprise Server latest update file (optional)
- Teramind Enterprise license key

Additionally, you can find instructional videos and other resources in the customer portal.

Server requirements

The following virtualization platforms are supported in production:

- VMWare ESXi 5.5 or later
- XenServer 6.5 or later
- Hyper-V

CPU and system memory should be provisioned based on the expected number of concurrent monitored sessions, according to the following table:

Concurrent Users	Cores	Memory
500 or less	8	8 GB
501 - 1000	16	24 GB
1001 - 2000	32	32 GB

The Teramind Enterprise virtual appliance comes with a primary volume of 24 GB. This volume contains the Teramind server application and database. The size of this volume can be increased at a later point in time.

Storage requirements

It is mandatory to add a second volume to the virtual appliance in order to store the screen recordings, among other things. This volume should be no smaller than 24 GB.

The simplest way to add storage is from your hypervisor, by simply adding a second volume. Teramind will automatically detect, format, and mount the volume once you add it to the virtual appliance. If you use Hyper-V, this volume should be a VHD file and not VHDX.

The size of this second volume can be estimated based on the number of sessions that will be recorded. With the default settings, for sessions with one screen doing normal work activity, you can expect approximately 1 GB per 160 hours.

You will be able to perform optimizations on recordings once the platform is deployed. For example, you can compress recordings by scaling down and converting to black & white, as well as recycle space by deleting old recordings based on some criteria.

Agent requirements

The Teramind Agent will run on the following platforms:

- Windows 7, 8, and 10 (32 & 64-bit)
- Windows Server 2008, 2012, and 2016
- OSX 10.7+, MacOS Sierra, MacOS High Sierra

The agent can be deployed on any of the following:

- Stand-alone computer
- Terminal Server
- Application / Session Server
- Citrix
- VDI

The Windows agent comes as two agents installer files – 32 and 64-bit. The same files can be deployed to any supported operating system / mode, as long as the architecture matches. You can obtain the agents at the customer portal or download them from the dashboard once your server is deployed.

Network requirements

Teramind Enterprise is suitable for deployment over LAN or WAN, even to remote sites with jittery internet connections. For your average, 1-screen session, average client-to-server network bandwidth requirement is approximately 10kb/s.

Teramind Enterprise also features offline recording. This means that in case of network downtime, the agent will save all data locally, and continue to enforce policy. Once connection is reestablished, the agent will upload the data to the server at a throttled pace.

Server deployment

Installing the virtual appliance

The Teramind virtual appliance can be used in three ways:

- Teramind Application server (default)
- Teramind screen mining node (optional)
- Teramind mining database node (optional)

The deployment procedures are the same for each type, and the same image is to be used. If you require screen mining functionality, remember that the virtual machines should be able to communicate with one another over the network.

Deploying on VMWare

1. Open vCenter or vSphere Client
2. Go to **File** => **Deploy OVF Template**
3. Select your Teramind Enterprise server image (.OVA file), as follows:

4. Accept all defaults by clicking **Next** until the VM is created

Deploying on XenServer or Hyper-V

Deploying on XenServer or Hyper-V is fairly similar to deploying on VMWare. The only change is that you should download and import the VHD image instead of the OVA.

Configuring the network

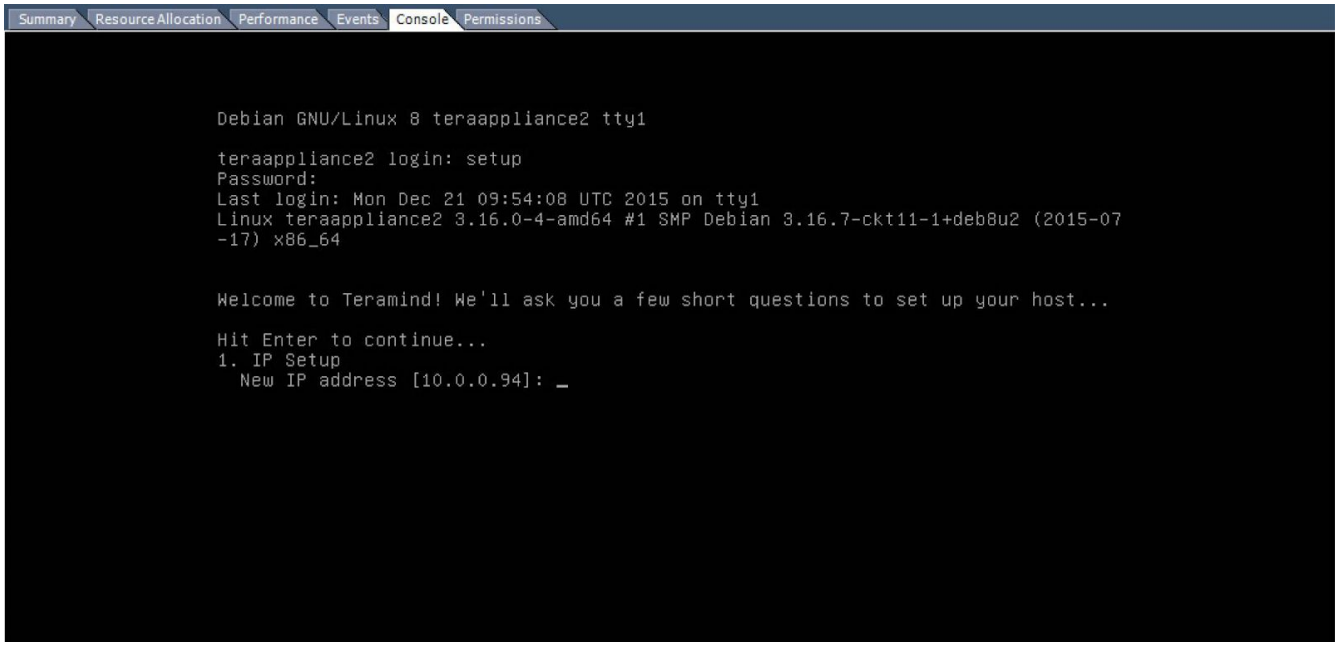
Configuring networking settings for the Teramind Enterprise virtual appliance is done via accessing the VM console.

1. Log in as using the following credentials:

   Username: setup

   Password: setup

2. Follow the menu and fill out the following information:
   - IP address
   - Netmask
   - Default gateway (optional)
   - Domain name server



Since this is a single-server deployment, select ‘master’ when prompted for the server role.

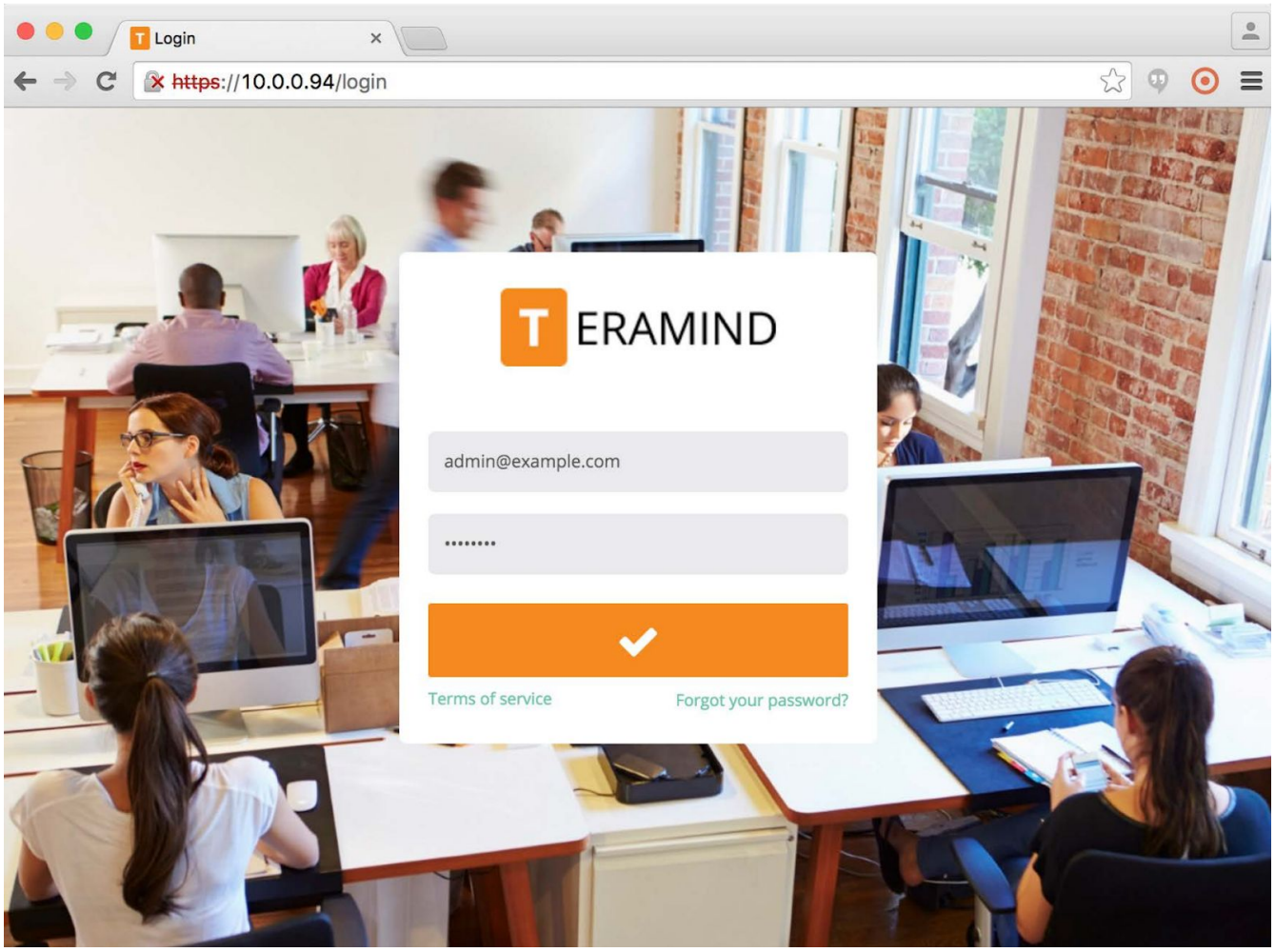
Accessing the Teramind deployment via browser

Access the dashboard from your browser by visiting the IP address of the VM and the following credentials:

Default username: admin@example.com

Default password: password

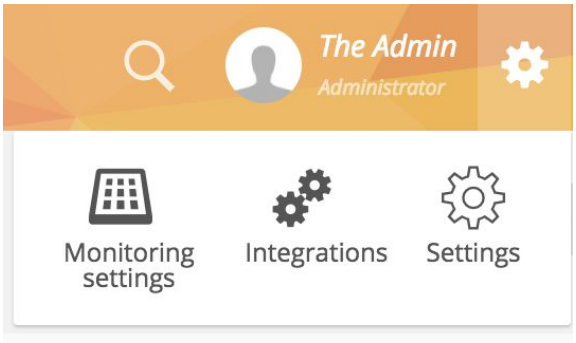
You can safely ignore any SSL warnings and proceed to the site.



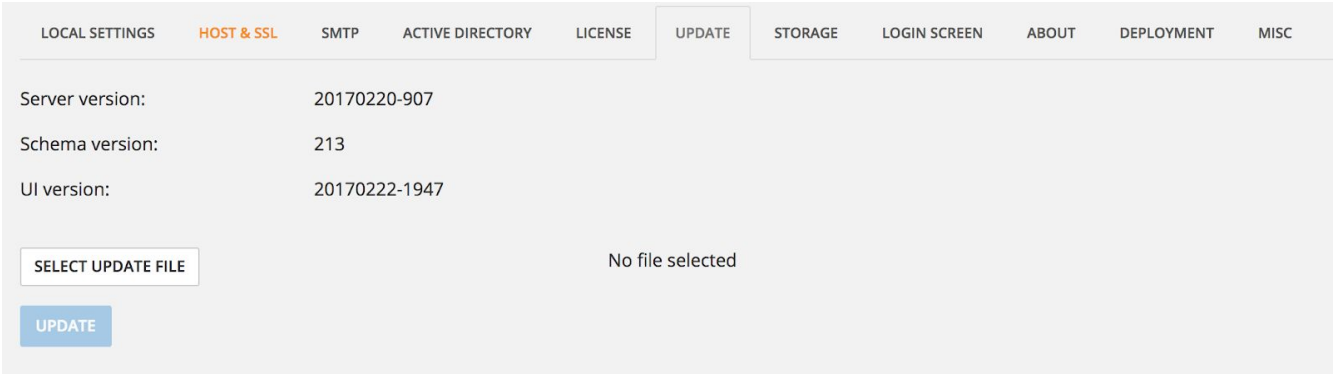
Server configuration

Configuration

Configuring Teramind is done entirely from the web-based dashboard. In the Teramind dashboard, hover over the cog on the top-right, and click on Settings.



You will be presented with a configuration menu as follows:



Licensing

Teramind Enterprise requires a valid license key to work. If you entered a valid license key when selecting the machine role, you can skip this step. Otherwise, to enter the license key which you were given, click on the License tab. Proceed to enter your license key, and click on Change. The system will display the entitlements for your license key.

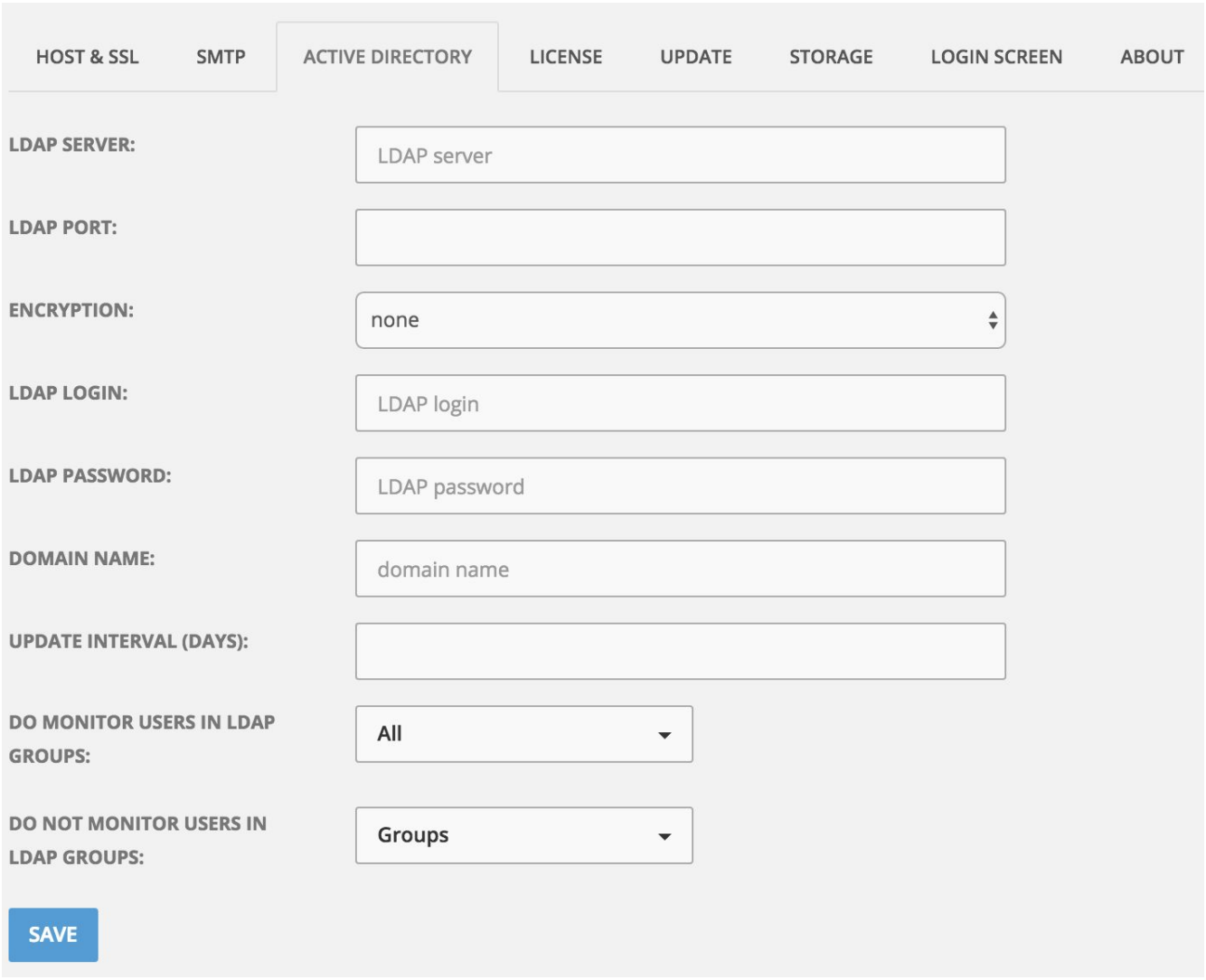
LDAP integration / Active Directory

Although not mandatory, LDAP integration will provide the following benefits:

- Synchronization of OU's and groups
- Synchronization of user accounts, OU and group membership
- Synchronization of computers and group membership
- The ability to report based on OU's
- The ability to apply rules to OU's and/or groups

- The ability to remote install to computers based on name, or AD group membership
- The ability to use Teramind only on a specific group
- The ability to exclude a group from being monitored

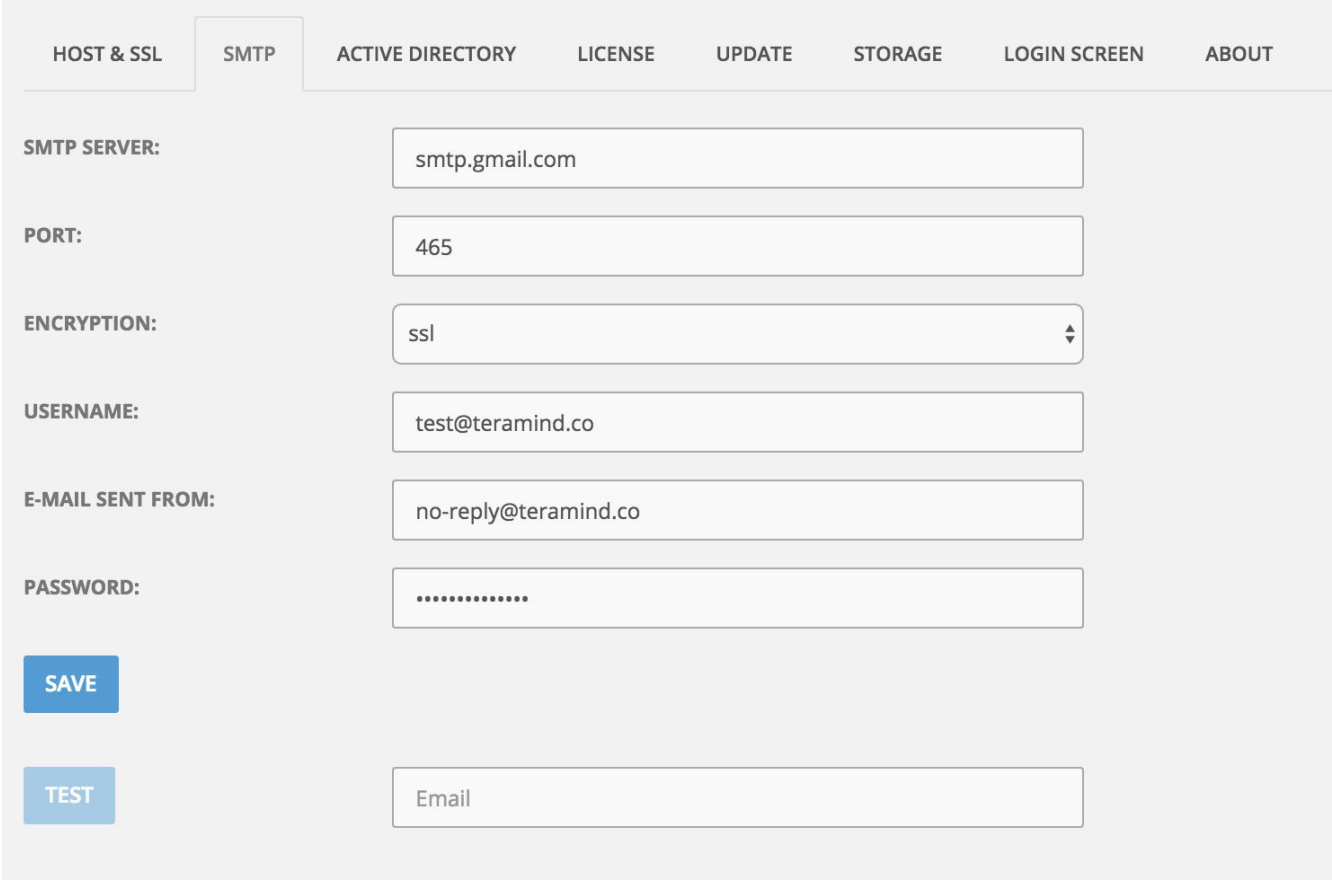
To configure LDAP, click on the Active Directory tab and populate the settings.



SMTP configuration

If you wish to receive alerts and system notification by e-mail, you must configure SMTP so that Teramind Enterprise can send out mail.

To configure SMTP settings, click on the SMTP tab and fill out the settings. Click on Save, and then Test once complete to ensure that the integration is successful.



SSL

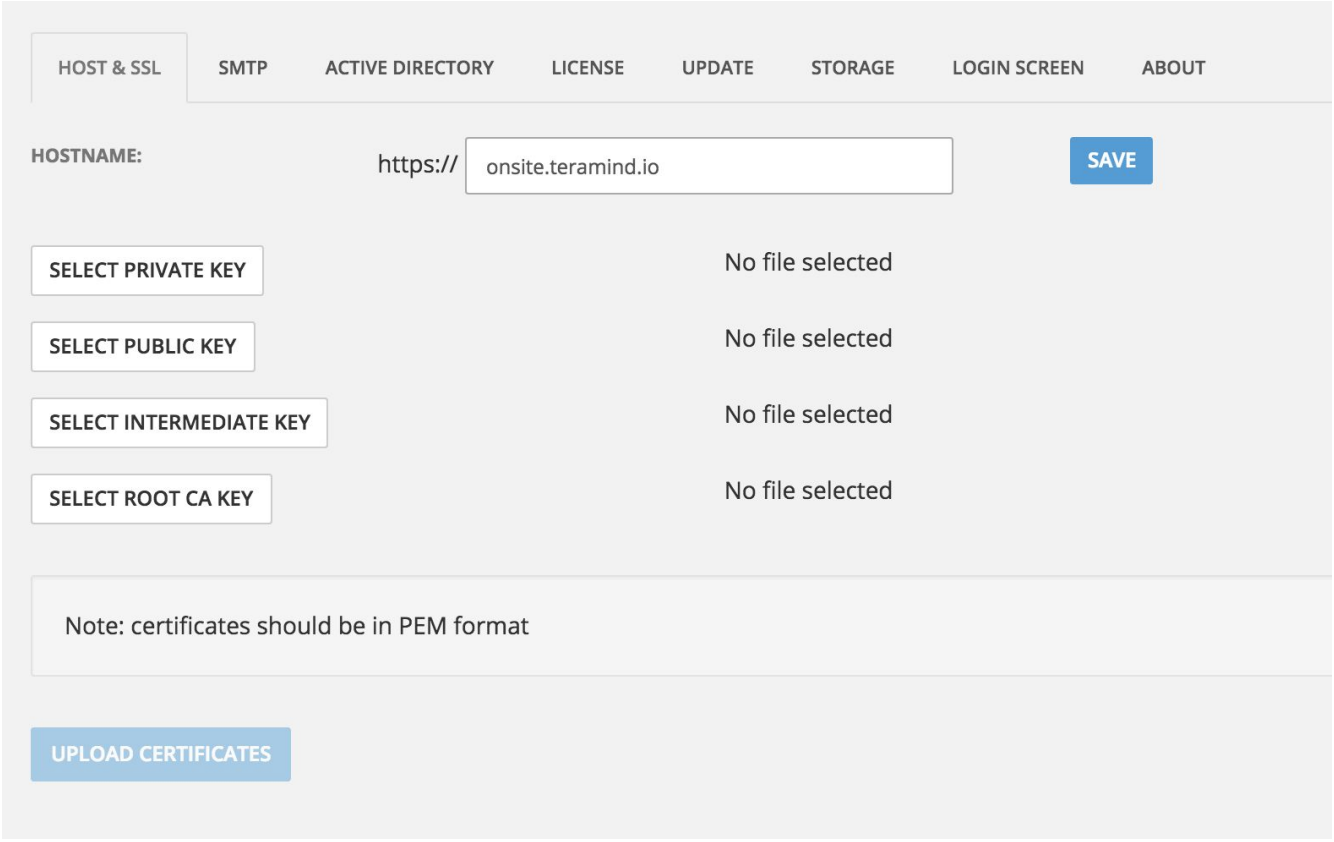
Teramind strongly recommends proper configuration of SSL in order to avoid browser warnings and restrictions. Some browsers will not allow websockets communications if the certificates are invalid. This may prevent you from watching live screens or screen recordings.

For convenience, Teramind comes pre-shipped with a SSL certificate that's valid for the hostname ***onsite.teramind.io***. If you wish to proceed without implementing your own certificates, you should add a line to your local hosts file and then access Teramind by browsing to https://onsite.teramind.io. You can do this by editing C:\Windows\System32\Drivers\Etc\hosts as Administrator and appending the following line to the file, where <ip-of-teramind> is the IP you assigned the virtual machine:

<ip-of-teramind> onsite.teramind.io

For the long run, you should deploy your organization's SSL certificates within Teramind, and add a DNS entry in your corporate name server for your Teramind implementation.

To enter your own certificates, click on the Host & SSL tab:



Certificates should be in PEM format. Enter your Teramind Enterprise appliance hostname, and upload the certificates as indicated in this form. After you're done, please access Teramind via the new hostname. You'll be asked to log-in again.

Screen mining setup

To set up screen mining you will need one screen mining database node and at least one screen mining node. These nodes will communicate with the master node and with each other.

Define the machine role

To configure a screen mining or screen mining database node, simply select the machine role when first setting up the IP address of the virtual appliance.

Approving the link

After setting the machine role and specifying the master node's IP address, open Settings => Deployment on the master node. You'll find the screen mining node approval request:

Click approve to link the two appliances together. Repeat for the screen mining database node. Screen mining will work if you have approved one screen mining database node and at least one screen mining node, and your license key supports screen mining.

Server update

If you've received an update file, the first thing you should do after server configuration is apply the update. It shouldn't take more than a few moments.

1. Select 'Update' from the tabs
2. Click on Select Update File, and select the *.TMU* update file that you received
3. Click on Update

The system will indicate when the update is complete.

Note: If you have deployed screen mining and screen mining database nodes, it is only necessary to update the master node. The remaining nodes will get updated automatically.

Agent deployment

Teramind Enterprise comes with two agents for Windows: 32 and 64-bit, and one agent for OSX / MacOS. The Windows agents are universal for any platform, including stand-alone workstations, and Windows Servers. There are several installation options which are applicable for different situations and have different degrees of complexity.

GUI installation

The simplest way to install the Windows or Mac agent is simply to double-click on the MSI or DMG from the endpoint which you wish to monitor. It will ask you only for the IP address (or hostname) of your Teramind Enterprise server.

Command-line installation (Windows)

MSIEXEC can be used in either command line (as Administrator) or from within a script, as follows:

C:\> ***msiexec /i //path-to/teramind/agent.msi TMROUTER=<ip-of-teramind>***

Where **<ip-of-teramind>** is the IP of the Teramind Enterprise appliance, and **//path-to/teramind/agent.msi** is either a URL, network, or local path to the Teramind agent MSI file.

Dashboard-based remote installation (Windows)

Teramind provides an easy-to-use interface for Windows agent installation in a domain environment. This method uses the same mechanism as PSEXEC or WMI, and requires the following:

- Ability to execute PSEXEC or WMI commands remotely (usually ports 135, 445)
- Domain administrator credentials

To use this functionality, open your Teramind dashboard. Hover over Configure in the left bar, and click on Computers. Click on ‘Remote Install Agents’ located at the top-right of the screen.

If you have successfully integrated LDAP in the previous section, you will be able to select computers by name and/or groups, and exclude computers by the same. You can also select computers by IP range.

Optionally, if your endpoints are able to access the internet, you can leave the URLs of the agent location as their default values. This will fetch the latest agent from Teramind. Alternatively, you can enter a local URL or network path to there the agents are located.

Finally, ensure that the domain administrator credentials, and IP address of the Teramind Enterprise appliance are correct. Once you click on Deploy you will be able to see the progress of your installation.

Antivirus considerations

The 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 will not introduce any issue with the vast majority of antivirus software. Nevertheless, you may want to add the following path to your Antivirus exception list as a precaution:

C:\ProgramData\{4CEC2908-5CE4-48F0-A717-8FC833D8017A}

C:\Windows\System32\drivers\tmfsdrv2.sys

C:\Windows\System32\drivers\tm_filter.sys

Firewall & proxy considerations

In most cases, you shouldn’t have to change any settings to get Teramind to work. The Teramind agents communicate with the Teramind Enterprise appliance on two ports: 443, and 10000. If you are monitoring audio as well, then the agent will connect to the server on some random UDP ports as well.

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. Note that for live and recorded screen playback, as well as live sessions 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.

Installation support & troubleshooting

We’re here to help. If you encounter any issues during your deployment, or have any questions, please contact your Teramind account representative for expedited assistance. You can also contact support@teramind.co.