Workshare Detect Server

Installation Guide

Table of Contents

Chapter 1: Introduction

This chapter introduces Workshare Detect Server, providing an overview of how it works and the system requirements for installation. It includes the following sections:

- **What is Detect Server?**, page 4, introduces Workshare Detect Server.
- **System Requirements**, page 5, describes the requirements for installation.

What is Detect Server

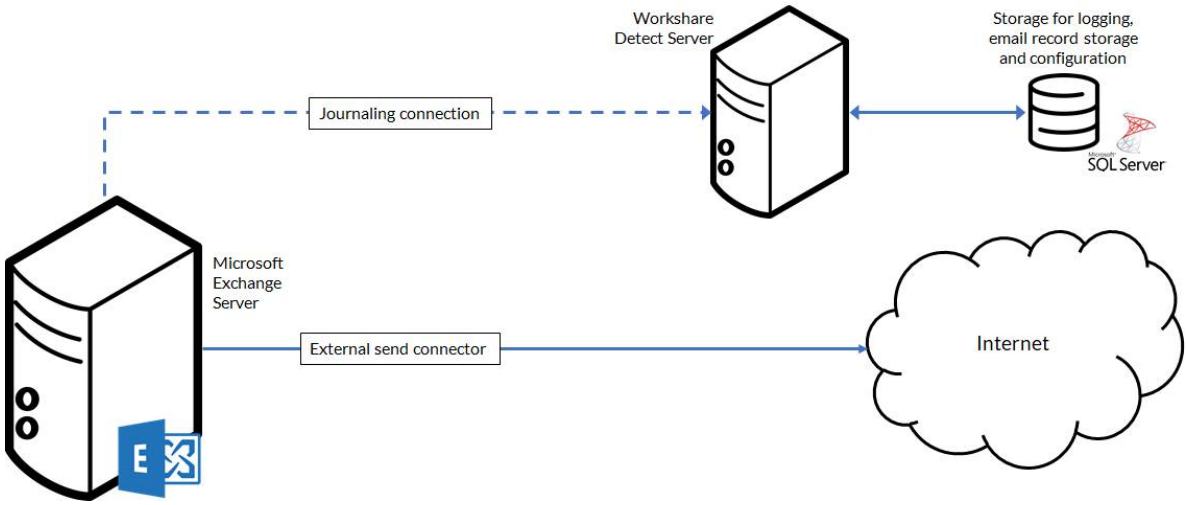
Workshare Detect Server enables compliance admins to monitor outgoing emails, giving them the information they need to analyze data security breaches. It does this by capturing a copy of all emails sent outside the company and storing information about every email and its attachments. Compliance admins can then run reports on the data, so they can analyze the information and implement policy accordingly.

For example, Detect Server stores information about all custom properties found in an attachment. This could be custom properties automatically added by a DMS or manually added by a user. Compliance admins can trace all documents sent out that included a specific custom property and identify who sent that document.

Comprehensive filtering of this large amount of data enables compliance admins to identify a problem, get to the root of it quickly and, consequently, react to data breaches promptly.

Detect Server is adaptable and configurable tackling data protection without risk to email flow:

- Monitor emails, without blocking
- React quickly to discover the source of data leaks
- Check the email activity of departing employees
- Comply with data protection regulations



Workshare Detect Server aims to provide a clear view into your firm's email traffic to allow you to recognize and flag anomalies and patterns of interest. The information gathered needs to be easily consumable, and Detect Server reports are being built into the product for ease of use.

In the current 1.7 release, one report (Free Domains) is included with Detect Server. All other reports will require the installation of Tableau Server.

System Requirements

Workshare Detect Server must be installed on its own dedicated server. The minimum specifications for the Detect Server machine are given below.

Hardware

Server class machine for Detect Server:

- 4 processing cores, 8GB RAM, 120GB HDD space

(optional) Server class machine to host Tableau Server:

- 4 processing cores, 16GB RAM, 250GB HDD space

(optional) Server class machine for document tagging:

- 2 processing cores, 4GB RAM, 120GB HDD space

Software

Server for Detect Server:

- Operating system: Microsoft Windows Server 2016 or 2012 R2
- Microsoft Exchange Server 2016 or 2013
- Microsoft SQL Server 2012 and above (2014 is recommended)

(optional) Server to host Tableau Server:

- Operating system: Microsoft Windows Server 2016 or 2012 R2
- Anaconda and Python 3.x
- Tableau (optional, for business intelligence)

(optional) Server for document tagging:

- Operating system: Microsoft Windows Server 2012 R2 Standard/Datacenter x64 Edition
- Worksmart DLPTagger from HBR Consulting

Prerequisites

The following software must be installed prior to the installation of Detect Server.

- Microsoft .NET Framework 4.5.2
- Microsoft Internet Explorer 11+

In addition, ports 80 and 443 must be open for web traffic on the Detect Server server.

Detect Server requires certain Windows features to be enabled. This is described as part of the deployment process in Step 1: Install prerequisites.

Database user credentials

The following users are required:

- **Database administrator**: The credentials for this user must be available prior to installation. The database administrator can be an SQL user or a Windows domain user, as long as they have a sysadmin role (or enough rights to create databases and assign users to databases). The database administrator user is required during installation to create database tables and to set up the processor user. These credentials are not stored after installation.
- **Detect Server processor user**: If using Windows authentication, the credentials for this user must be available prior to installation. If using SQL authentication, the installer will create a user (with database read and write permissions to the Detect Server database) if one doesn't exist. The processor user should have a "public" role only and cannot be the same user as the database administrator. This user is to enable communication between Detect Server and the database and would typically only be given minimum access permissions (to the Detect Server database catalog only). These credentials are stored on the Detect Server machine.

Chapter 2: Deployment

This chapter describes how to deploy and set up Workshare Detect Server in your environment. It includes the following sections:

- **Installation Files**, page 8, describes the files included in the Detect Server installation bundle.
- **Deploying Detect Server**, page 8, describes each step of the deployment process.

Installation Files

The following files are included in your Workshare Detect Server installation bundle:

- Detect-server-installer- [version number].exe
- install-detectserver-prerequisites-win2012-2016.ps1

You should save these files locally. For the installation described in this guide, the files have been saved to C:\WDSInstall.

***Note**: You will also receive a LIC file to license Detect Server.*

On your Detect Server machine, you install the Windows prerequisites, configure SMTP server and then install the Detect Server executable. You will also have to perform some configuration on Exchange.

Upgrading

Detect Server does not support upgrades from earlier versions. You must uninstall previous versions and then repeat step 3 below to install Detect Server 1.7. Databases will be migrated automatically.

Deploying Detect Server

The installation and setup of Workshare Detect Server includes the following steps:

Step 1: Install prerequisites

Step 2: Configure SMTP server

Step 3: Install Detect Server software

Step 4: License and check the Detect Server machine

Step 5: Configure Exchange

(optional) Step 6: Custom property stamping on documents

(optional) Step 7: Business intelligence reporting

Follow these steps in the order shown.

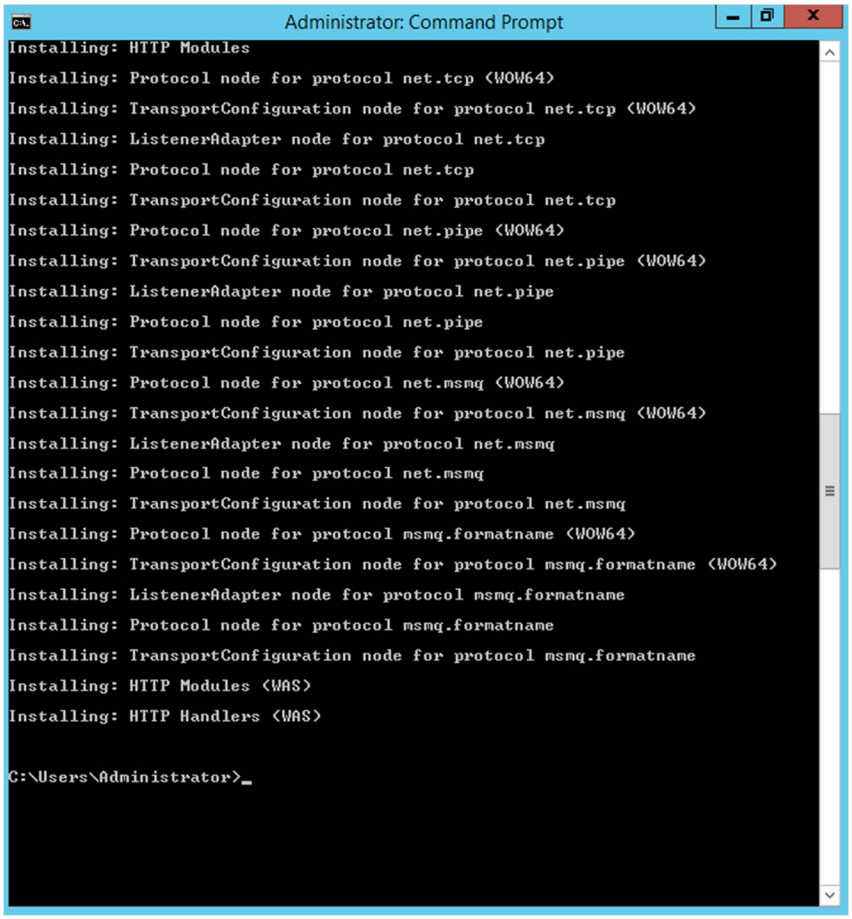
Step 1: Install prerequisites

Windows prerequisites

A PowerShell script (**install-detectserver-prerequisites-win2012-2016.ps1**) is included with the installation to add the Windows features required for Detect Server.

To install the Windows prerequisites:

1. On your Detect Server machine, open a command prompt as administrator.
2. Type: `@powershell -ExecutionPolicy Bypass -Command "C:\WDSInstall\install-detectserver-prerequisites-win2012-2016.ps1"`
3. Press Enter on your keyboard. This command checks permissions and runs the PowerShell file to install the required Windows features. Once complete, you will see:



> ***Note**: If there is a "the source files could not be found/downloaded" error, run the procedure described here: https://technet.microsoft.com/en-GB/library/dn482071.aspx*

Runtime prerequisites

If you're working on a server without internet access, ensure the following three redistributable packages are installed before installation of Detect Server. If your server has internet access, Detect Server can install these prerequisites during installation.

- **Microsoft Visual C++ 2005 Service Pack 1 Redistributable Package ATL Security Update**

  The executable file is downloaded by clicking this link: http://download.microsoft.com/download/6/B/B/6BB661D6-A8AE-4819-B79F-236472F6070C/vcredist_x86.exe

- **Microsoft Visual C++ 2008 Service Pack 1 Redistributable Package ATL Security Update**

  The executable file is downloaded by clicking this link: http://download.microsoft.com/download/9/7/7/977B481A-7BA6-4E30-AC40-ED51EB2028F2/vcredist_x86.exe

- **IIS URL Rewrite**

  The executable file is downloaded by clicking this link: http://download.microsoft.com/download/6/7/D/67D80164-7DD0-48AF-86E3-DE7A182D6815/rewrite_2.0_rtw_x64.msi

Step 2: Configure SMTP server

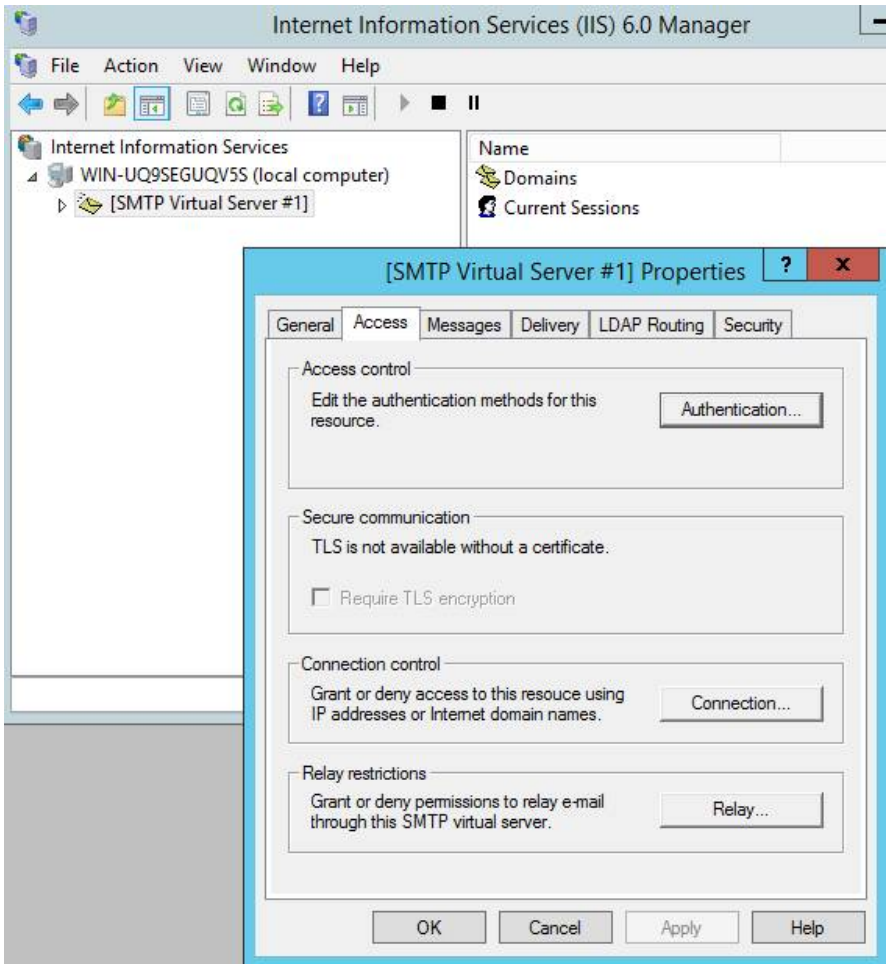
The SMTP server on the Detect Server machine receives the journaled email (copies of emails) from Exchange Server. This step is to configure the SMTP server to accept emails from your Exchange environment.

By default, Detect Server consumes emails that have been processed so the SMTP server will not relay them on for delivery. However, as added security to ensure emails are not relayed unintentionally, this step also configures SMTP server to accept emails and not relay them further.

In order to configure the SMTP server, you need to decide on the journaling email address. This should be unique for your organization. For the installation described in this guide, the journaling email address used is **journal@worksharedetectserver.local**.

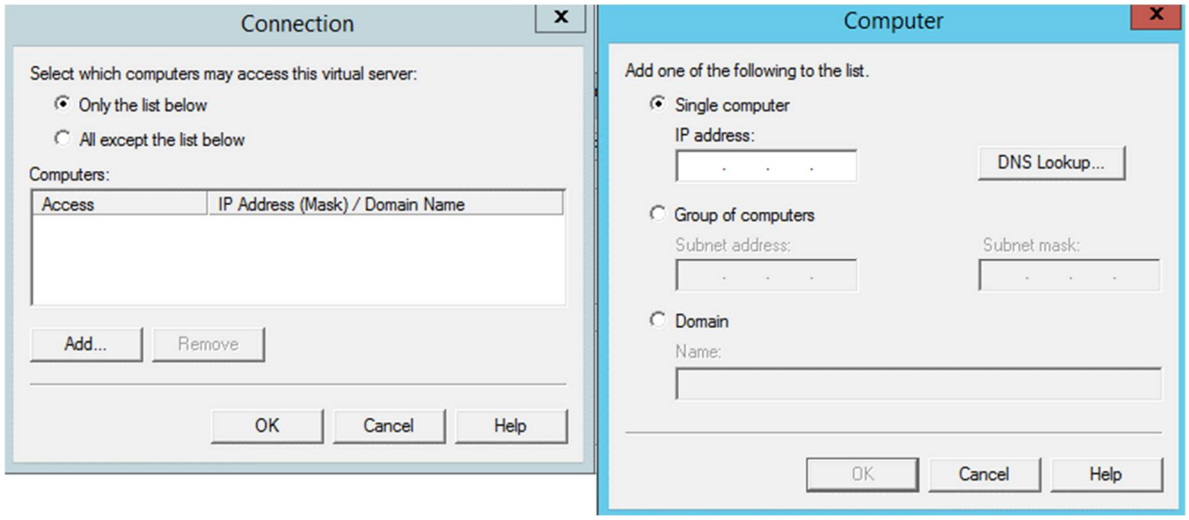
To configure the SMTP server:

1. On your Detect Server machine, open Internet Information Services (IIS) 6.0 Manager.
2. Open SMTP server properties.
   - Expand the local computer.
   - Right-click **[SMTP Virtual Server #1]** and select **Properties**.

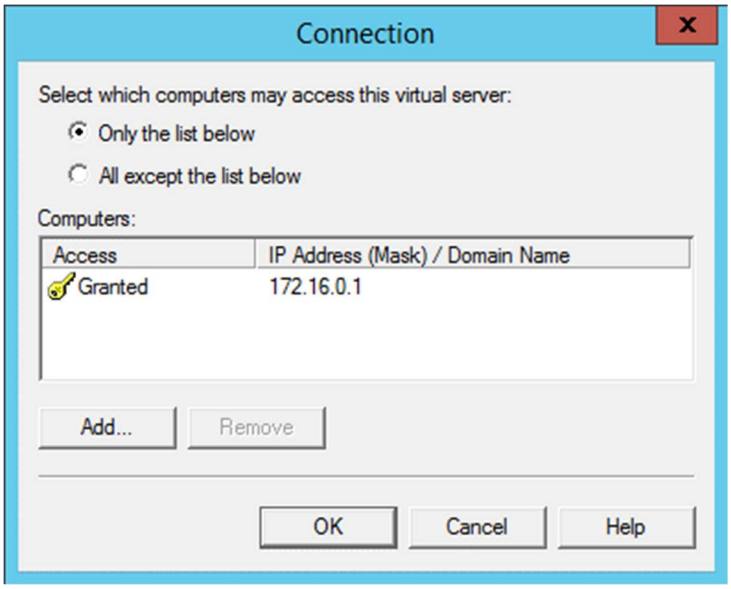


3. Select the **Access** tab.

4. Add a connection rule to allow Exchange servers to connect to the SMTP server on the Detect Server machine.
   - In the **Connection control** area, click **Connection**.
   - Select **Only the list below**.
   - Click **Add**.



   - Select **Single computer**.
   - Enter the IP address of your Exchange server.
   - Click **OK**.



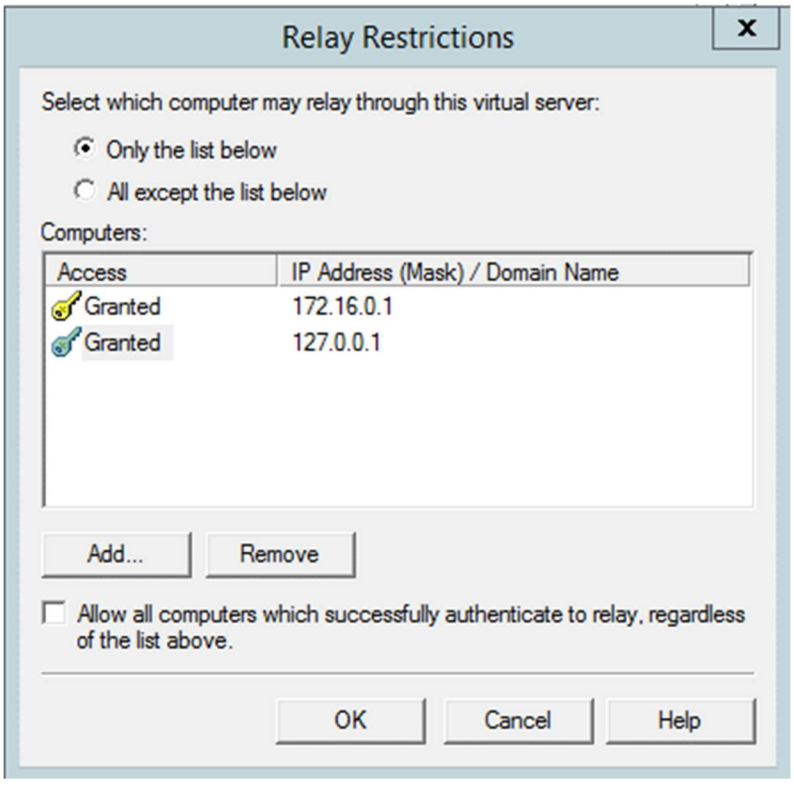
***Note**: Repeat this process if you have more than one Exchange server so you have the IP addresses of all of them listed in the Connection dialog.*

   - Click **OK**.

5. Add a relay rule to allow Exchange servers to relay to the SMTP server on the Detect Server machine.
   - In the **Relay restrictions** area, click **Relay**.
   - Select **Only the list below**.
   - Click **Add**.
   - Select **Single computer**.
   - Enter the IP address of your Exchange server.
   - Click **OK**.

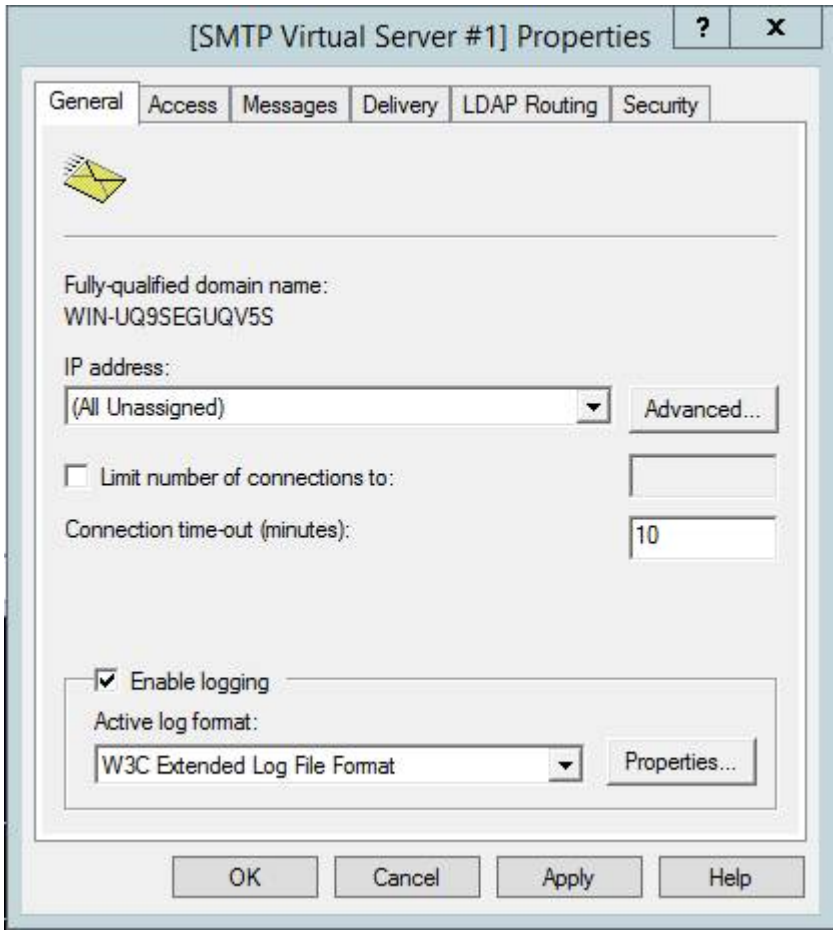
> ***Note**: Repeat this process if you have more than one Exchange server so you have the IP addresses of all of them listed in the Connection dialog.*

6. Add a loopback address to allow Detect Server to send to itself, for example, password reset emails.
   - Click **Add**.
   - Select **Single computer**.
   - Enter the IP address 127.0.0.1 to ensure that Detect Server can send password reset emails.
   - Click **OK**.



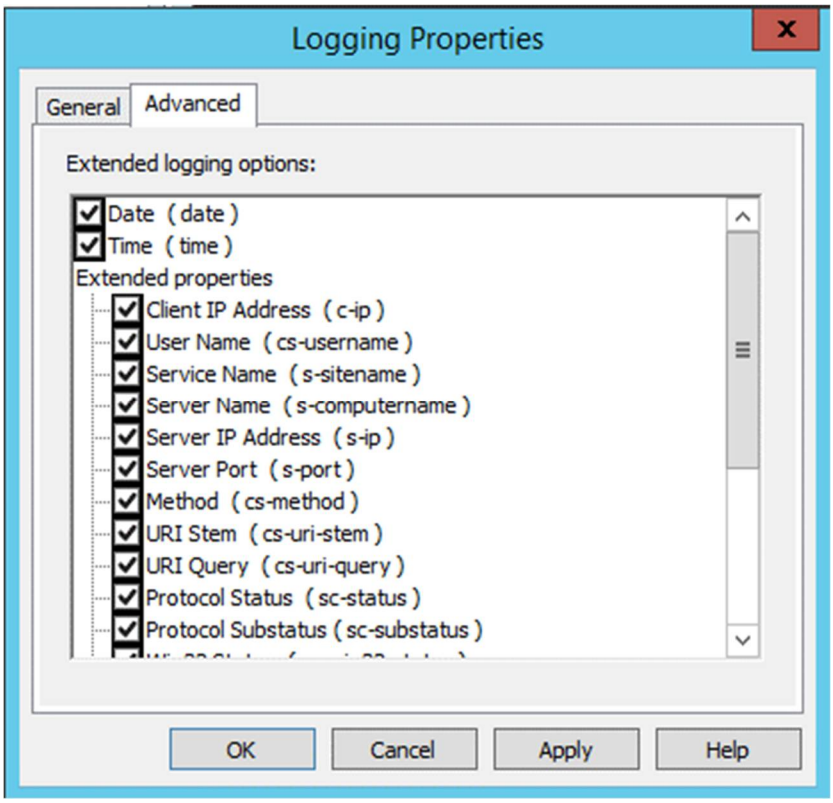
7. Click **OK** in the Relay Restrictions dialog.
8. Select the **Messages** tab.

9. Set the message size parameters to match your organizational limit.
10. Select the **General** tab.



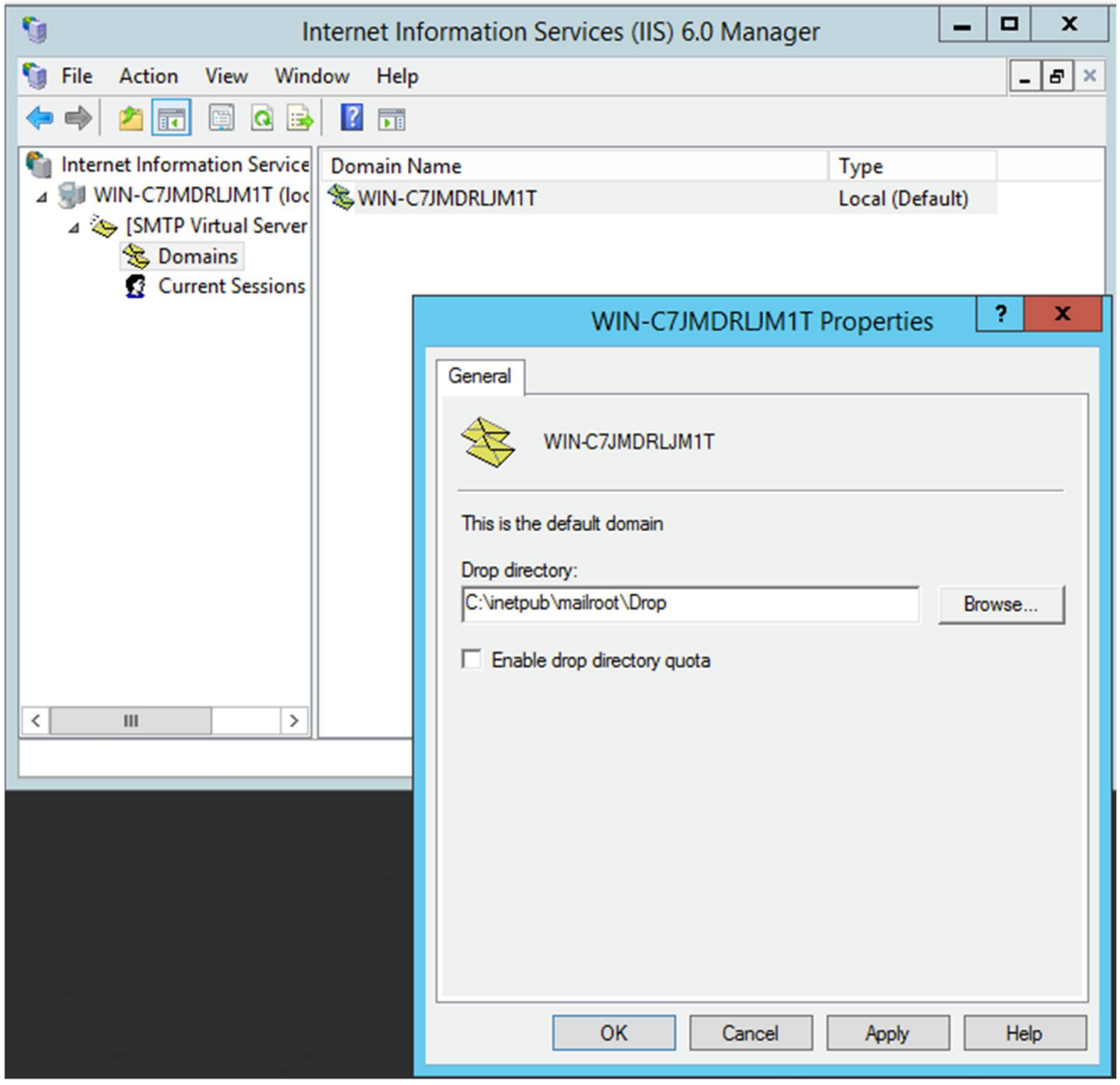
11. Select **Enable logging** and click **Properties**.

12. Click **Advanced** and select all of the extended properties.



13. Click **OK**.
14. Click **OK** in the Properties dialog.
15. Right-click the **Local (default)** domain, and select **Properties**.

16. Ensure that the **Enable drop directory quota** checkbox is NOT selected.

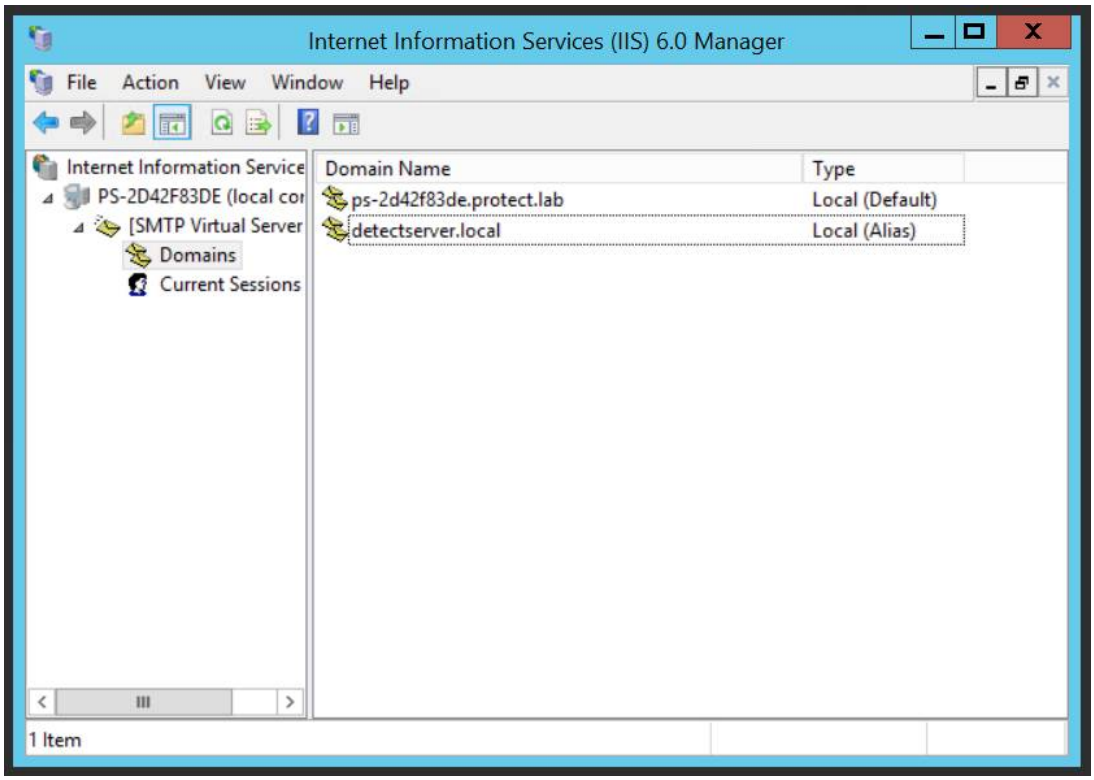


17. Click **OK**.

18. Set up a new SMTP domain with the domain of your journaling email address.
    - Right-click in the blank space on the right and click **New > Domain**.
    - Select **Alias** as the domain type.
    - Click **Next**.
    - Enter the domain name of your journaling email.

***Note**: The recommended journaling domain is **worksharedetectserver.local**. This will avoid real outbound email from being routed to the Detect Server machine.*

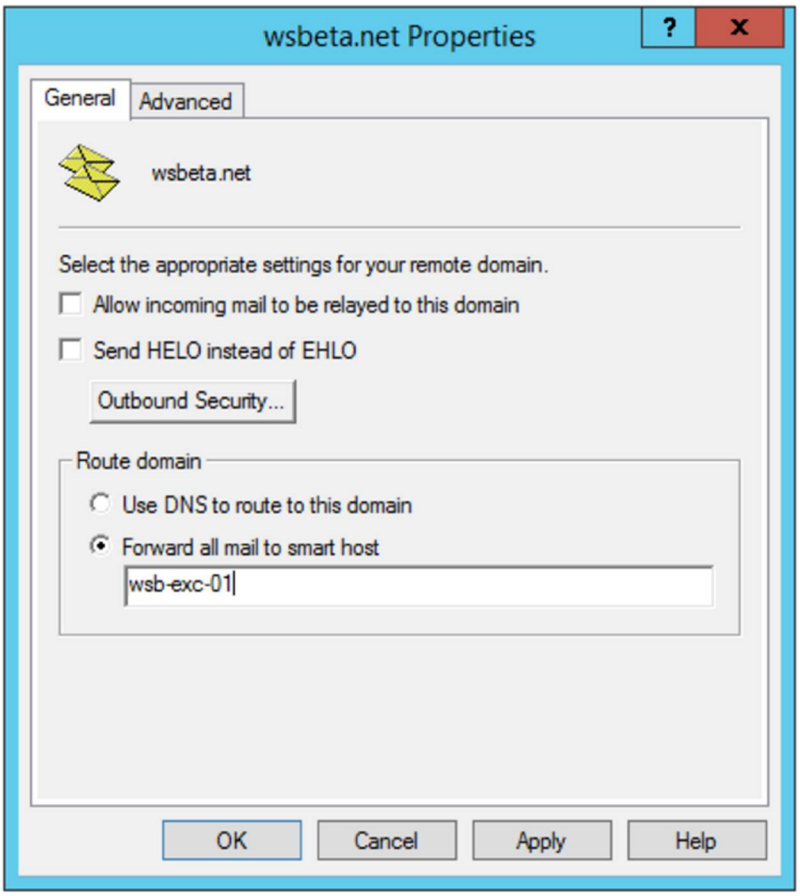
- Click **Finish**.



19. Create a route for user management emails back to your Exchange server.
    - Right-click in the blank space on the right and click **New** > **Domain**.
    - Select **Remote** as the domain type.
    - Enter the email domain used by the email addresses of the administrators of Detect Server.

> ***Note**: If there is more than one email domain to manage, then these need to be configured in the same manner.*

- Once the domain has been created (wsbeta.net as an example), right-click and select **Properties**.



- In the **Route domain** section of the **General** tab, select **Forward all mail to smart host**. Enter the address of the Exchange server that the email for that email domain is to be delivered to (wsb-exc-01 as an example).

Step 3: Install Detect Server software

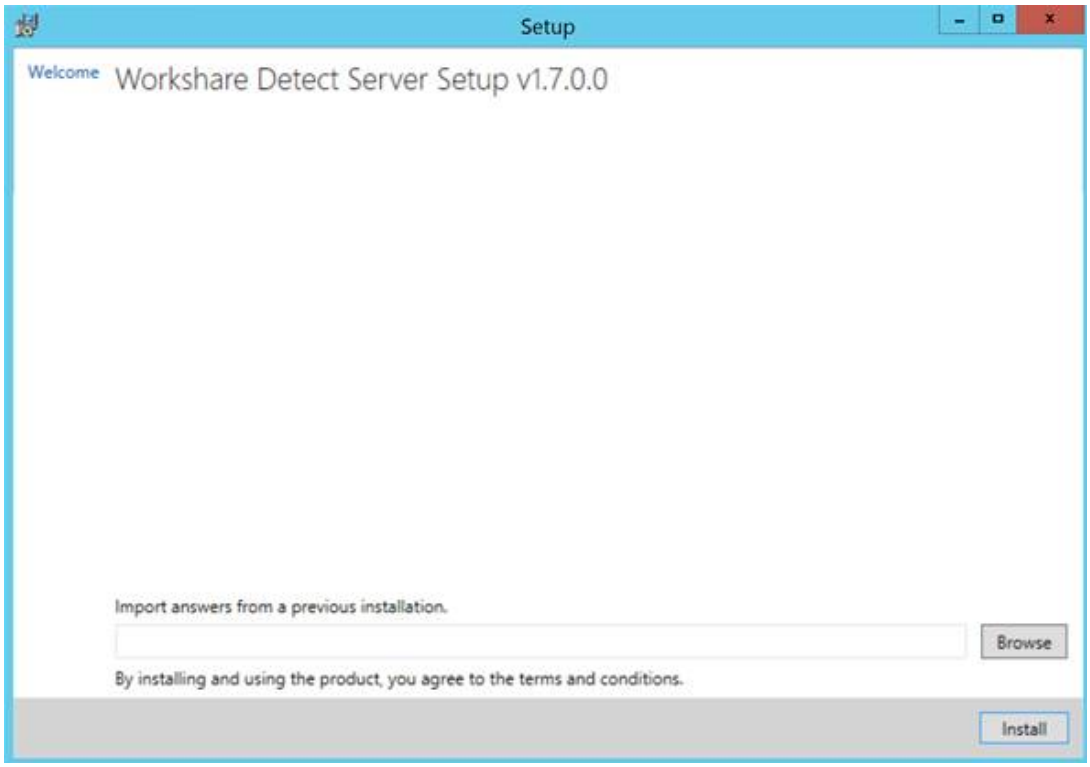
In this step, you run the Detect Server executable. During the installation, you will be prompted to enter:

- Database details.
- API keys. These secure the REST API that is used by the Mail Transport Agent (MTA) and potentially other future web services.
- A location to save unprocessable emails.

This step in the installation process normally takes between 2 to 5 minutes.

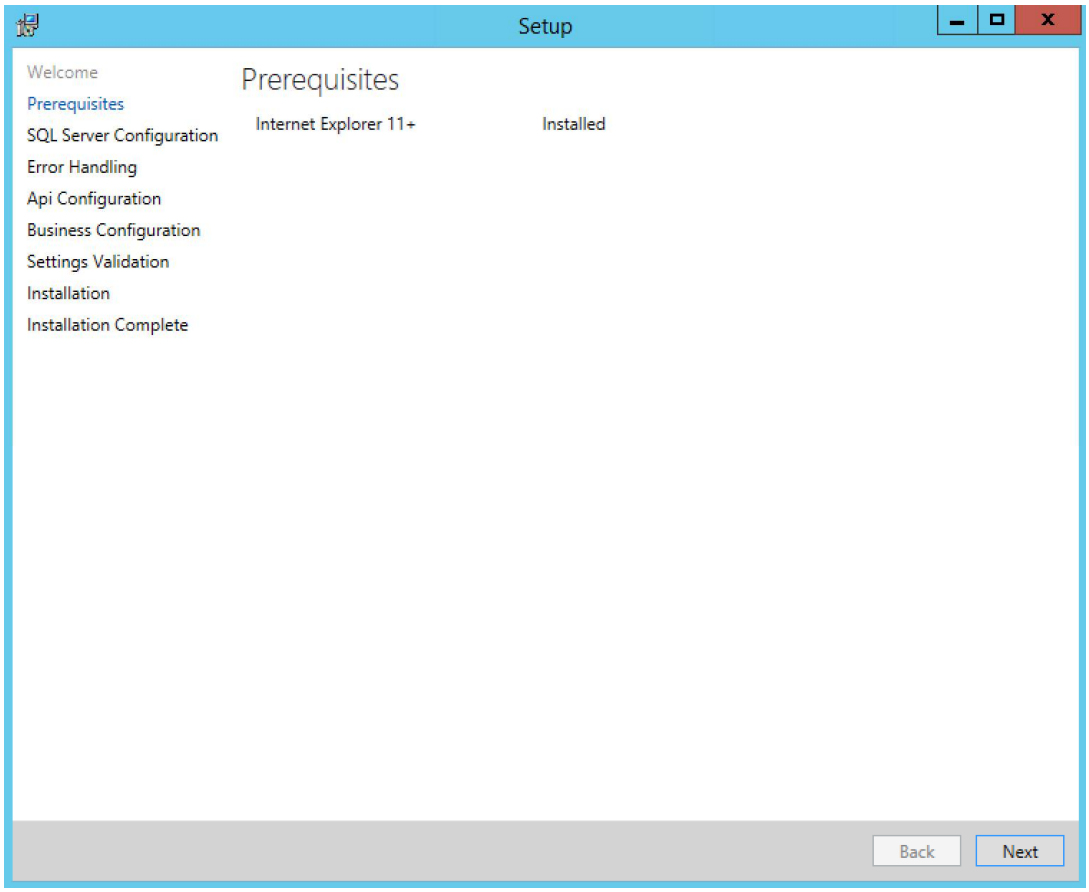
To install the Detect Server software:

1. On your Detect Server machine, run the Detect Server executable.

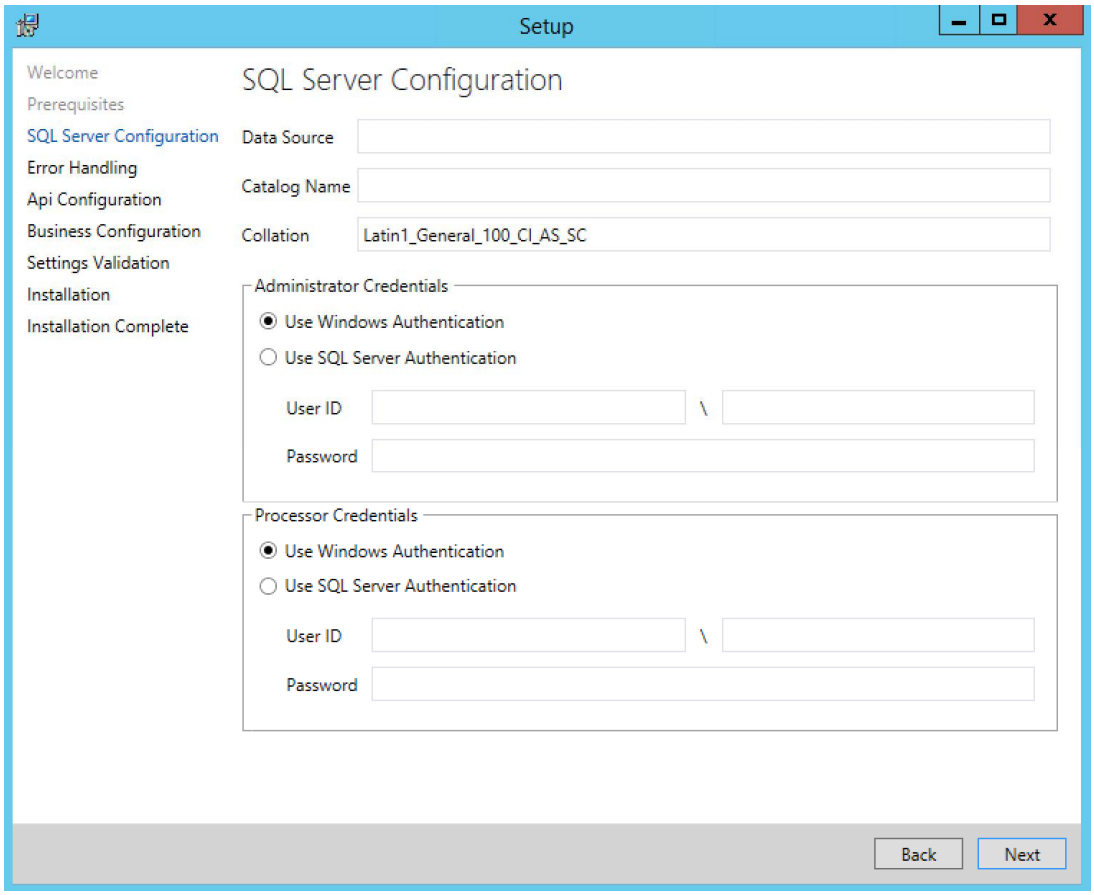


***Note**: Every installation creates an answer file that can be re-used in subsequent installations. You may provide an answer file containing previously entered configuration if available and applicable. You will need to re-enter passwords.*

2. Click **Install**. The Prerequisites page is shown confirming whether the prerequisites are installed.

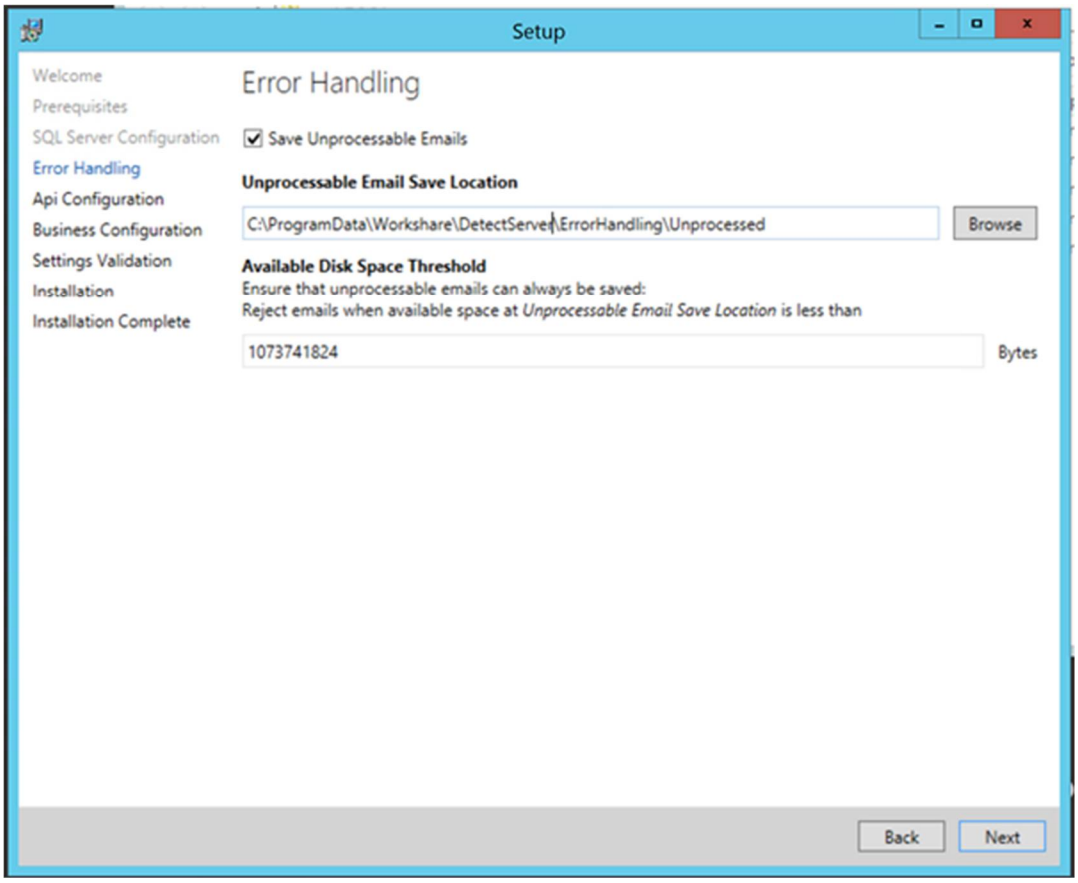


3. Click **Next**.



4. In the **Data Source** field, enter the location of your database. This is the IP address or host name of your SQL server.
5. In the **Catalog Name** field, enter a name for your Detect Server catalog in your database, for example, RADB.
6. The **Collation** controls the rules by which strings are sorted by in the database so you might need a different collation when using a foreign language. The default collation for Detect Server should be good for western European countries. If your SQL administrator has configured a default collation for the SQL server, you should leave this field blank.
7. In the **Administrator Credentials** area, enter the details for your administrator user (described in Database user credentials).
8. In the **Processor Credentials** area, enter the details for your processor user. If you select **Use SQL Server Authentication**, the user will be created if the user doesn't already exist.

9. Click **Next**.

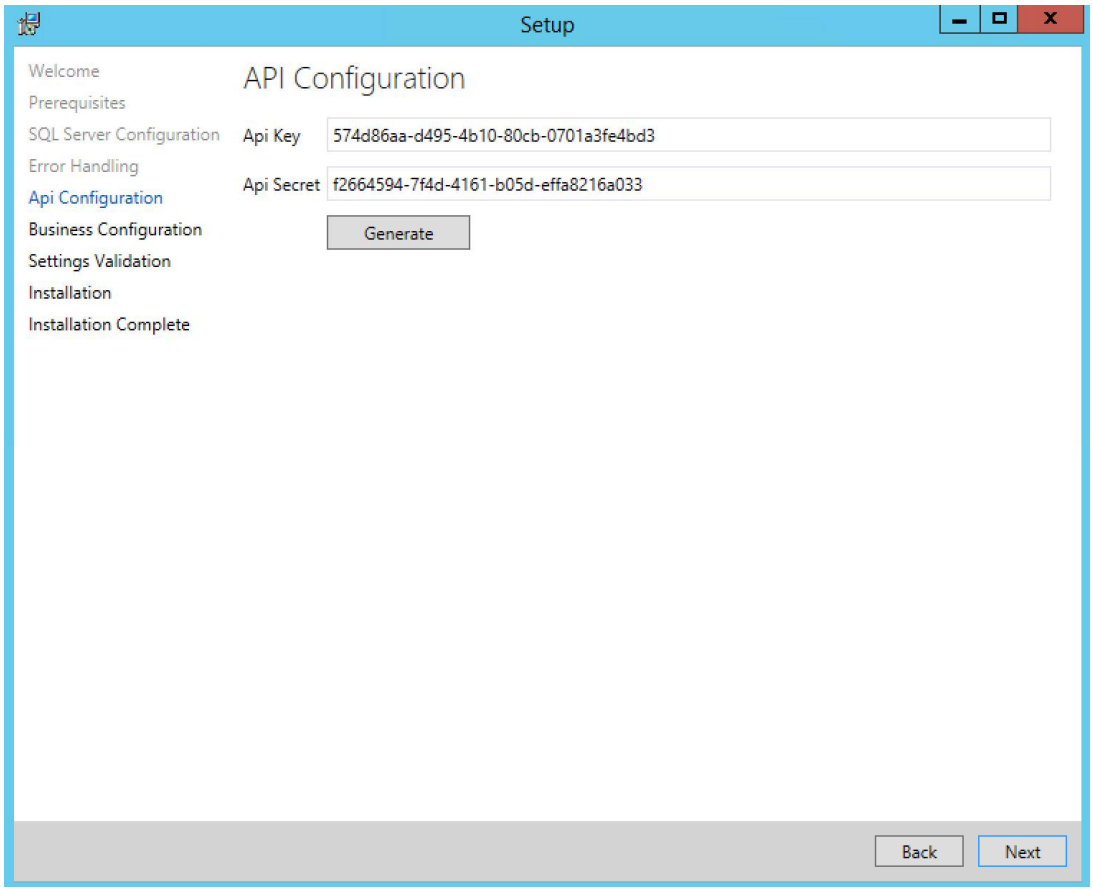


10. Select **Save Unprocessable Emails**. This means that if there are email journals that Detect Server cannot process, it will save them in the location shown. Click **Browse** and change the location if required.

11. Leave the **Available Disk Space Threshold** as the default of 1073741824 bytes (1 gigabyte). This means that if there is less than 1 gigabyte of space in the **Unprocessable Email Save Location**, Detect Server will reject the email journal and it will sit in a queue in Exchange waiting.

> ***Note**: Exchange will route the email journal to another Detect Server machine if one is configured.*

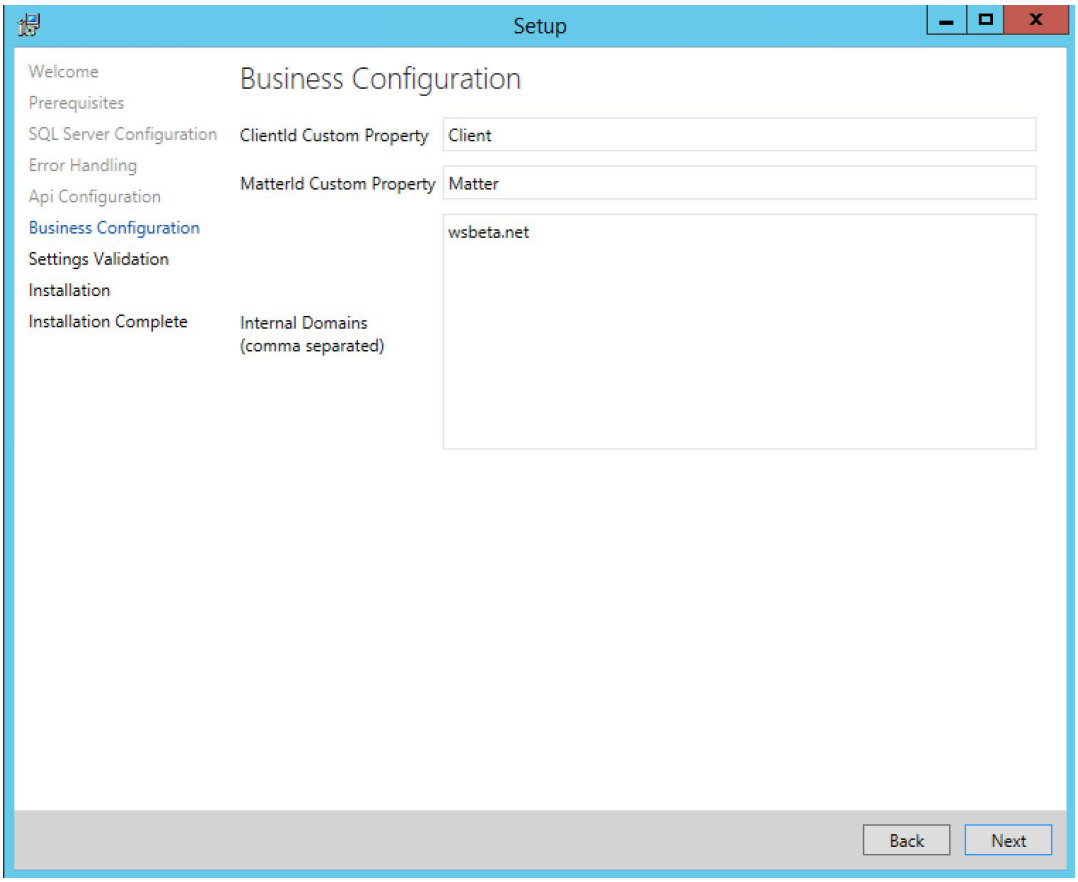
12. Click **Next**.



13. In the API Configuration page, click **Generate** to generate a random set of keys that will secure access to the Detect Server API.

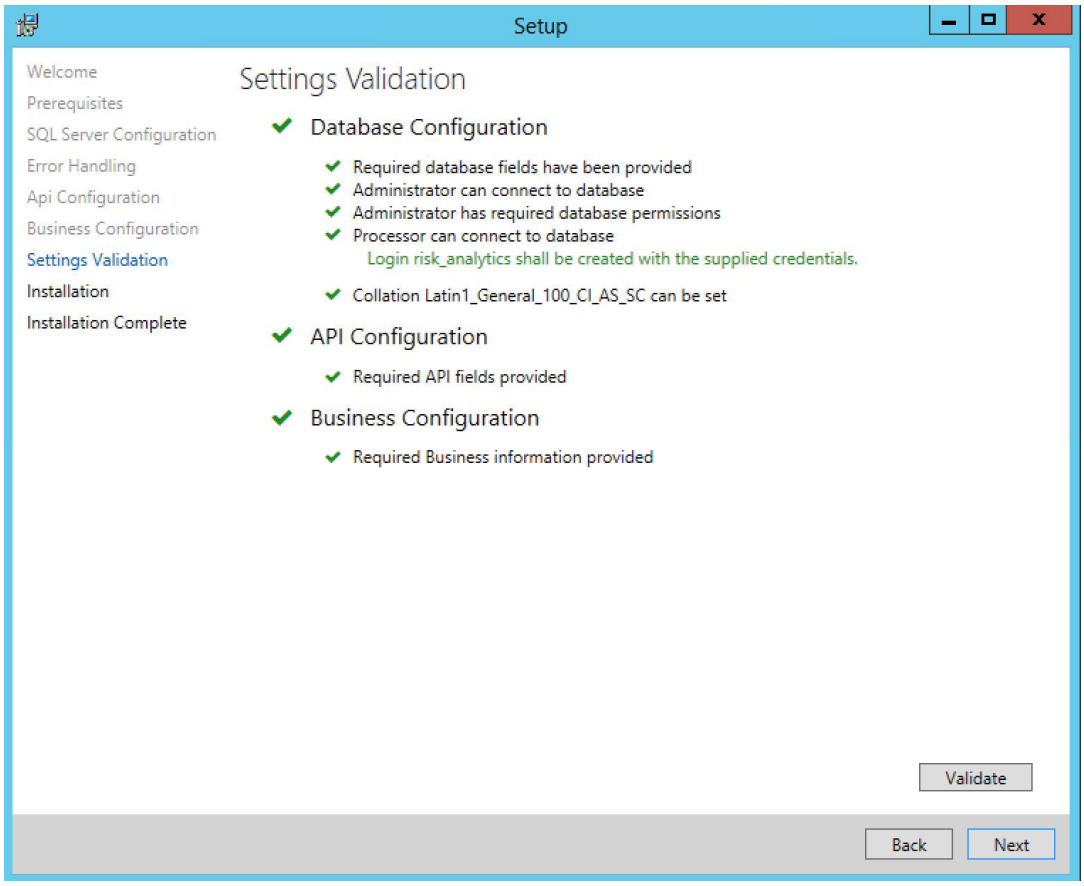
> ***Note**: If you are installing multiple instances of Detect Server, the same API key and secret should be used for each one.*

14. Click **Next**.



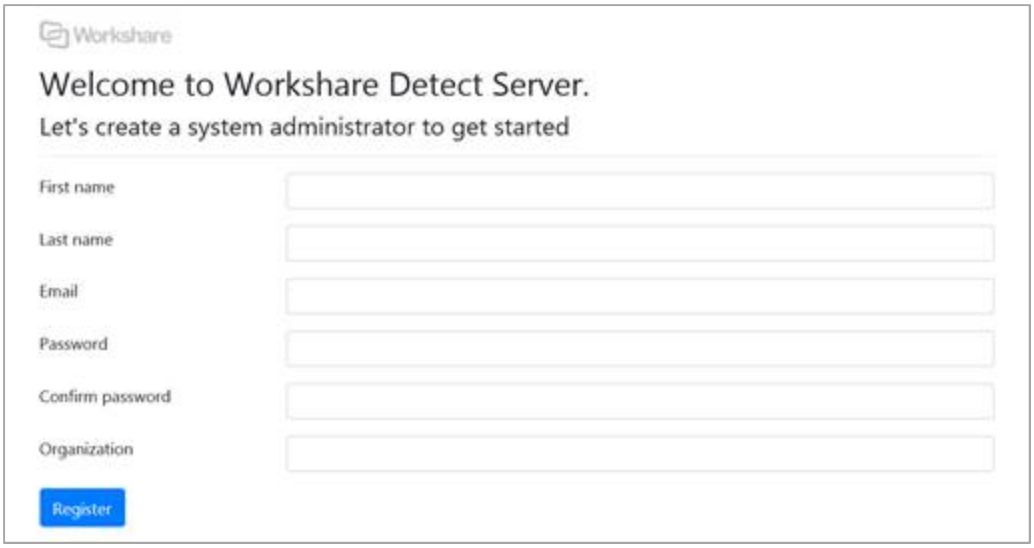
15. In the **ClientId Custom Property** and **MatterId Custom Property** fields, enter the custom property (key) you use to identify clients and matters. Detect Server will monitor these keys and record their values.
16. In the **Internal Domains** field, enter your internal domains so that Detect Server can identify which emails are going to internal recipients.
17. Click **Next**.

18. In the Settings Validation page, click **Validate**.



19. Click **Next**. Detect Server is installed. This process may take several minutes.
20. Once the installation is complete, click **Next**.

21. Click **Launch Detect Server**. Your browser opens showing the login page.



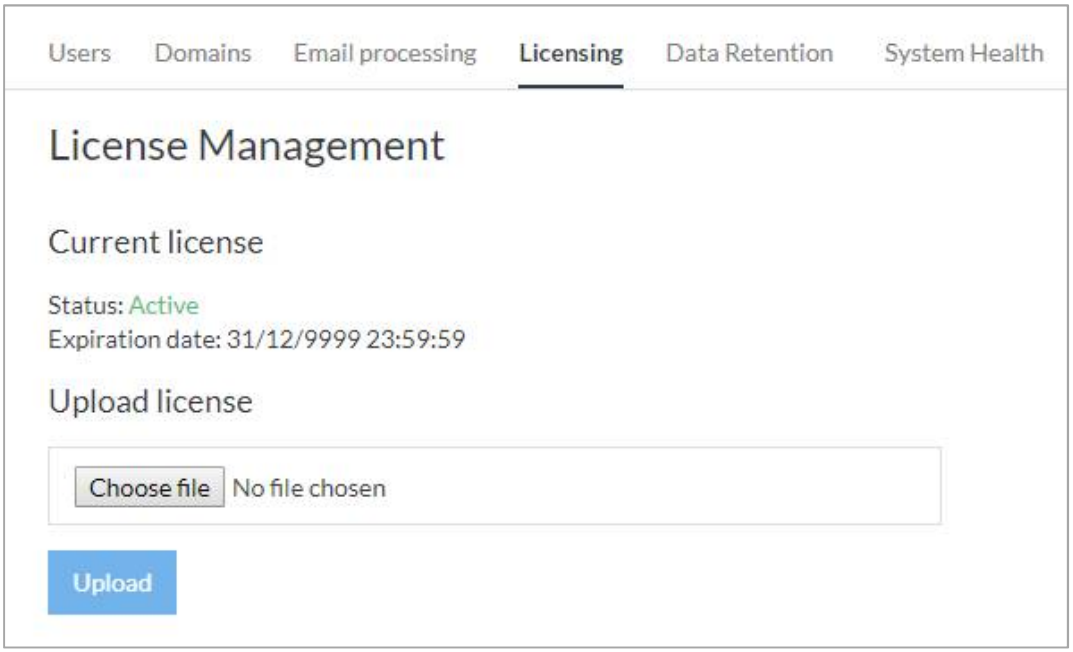
22. Enter your name, organization and email, and set a password. You will be the first administrator user for Detect Server. You can add further administrator users later – see Inviting Users.
23. Click **Register**. The Detect Server console is displayed.

Step 4: License and check the Detect Server machine

You will need the LIC file provided by Workshare to license Detect Server.

To license Detect Server:

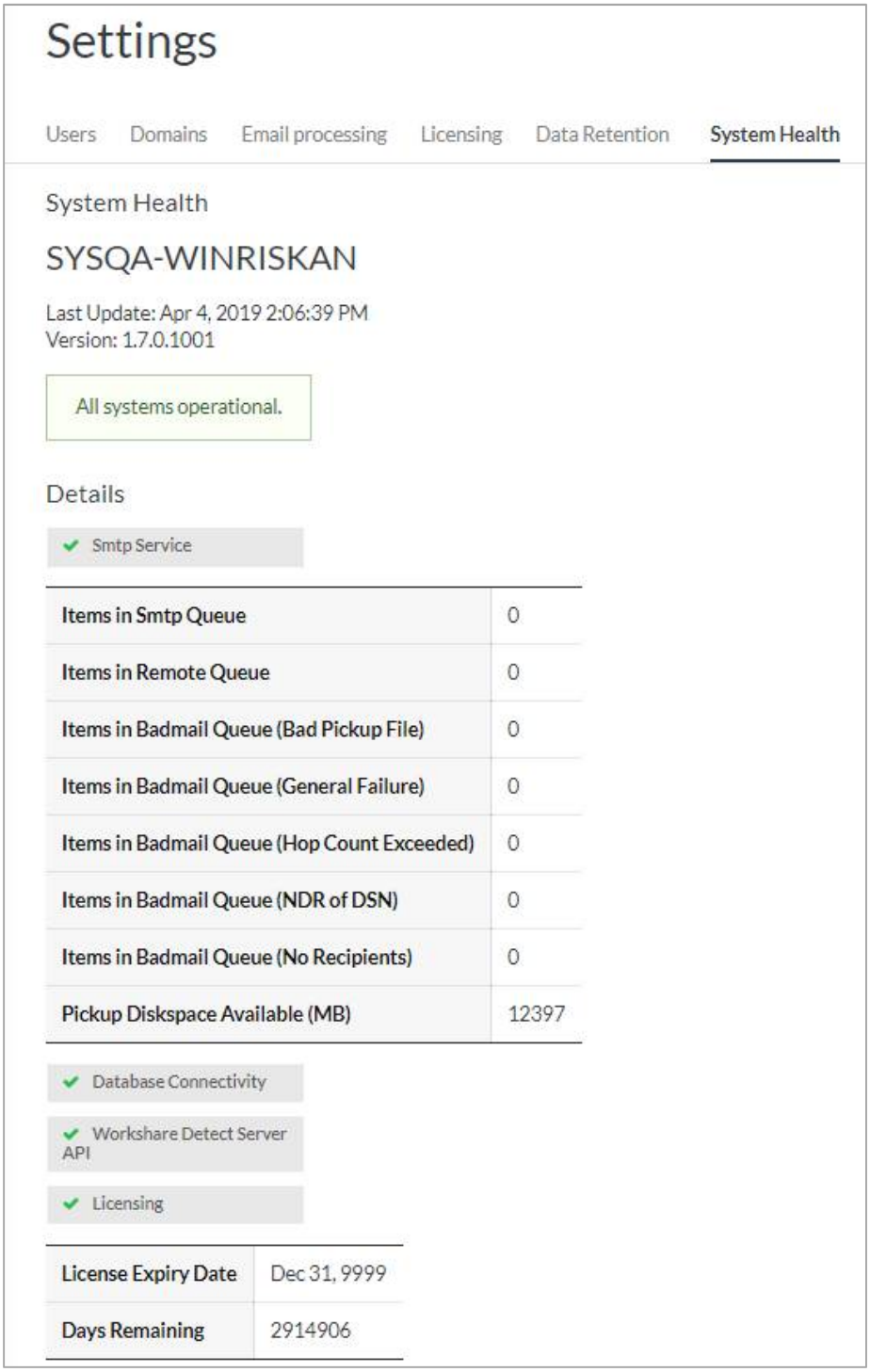
1. Log into the Detect Server console, click the Settings icon and then select the **Licensing** tab.



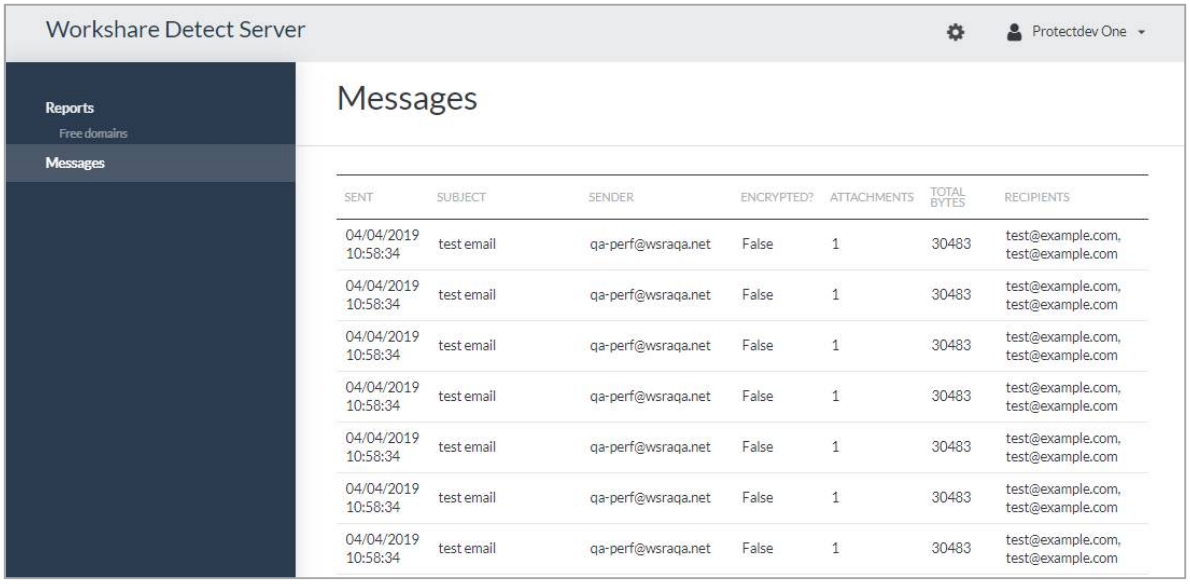
2. Click **Choose file** and browse to the saved LIC file provided by Workshare.
3. Click **Upload**.

You can check your deployment was successful by following the steps below.

1. Log into the Detect Server console, click the Settings icon and then select the **System Health** tab and watch for all the lights to go green.



2. In the Detect Server console, select **Messages**. You should see email results appear.



Step 5: Configure Exchange

On Exchange, you must create send and receive connectors and a journal rule so that copies (journals) of all emails are sent to Detect Server.

***Note**: The recommended journaling domain is **worksharedetectserver.local**. This will avoid real outbound email from being routed to the Detect Server machine.*

The procedure may vary according to your Exchange version. The following procedures describe how to create a send connector, a receive connector and a journal rule from the command line which is the same on all versions of Exchange.

Create a send connector

Add a send connector for Detect Server with the following details:

- Address space: <your .local journal domain>
- Smart host: [IP address or FQDN of Detect Server machine]

To create a send connector:

1. Open Exchange PowerShell (also known as the Exchange Management Shell.
2. Enter the following command:

```
new-sendconnector -custom -name "Detect Server" -AddressSpaces
worksharedetectserver.local -SmartHosts "[<your detect server ip
address>]"
```

This creates a basic send connector. You may also need to modify your send connector for authentication, message size limits, additional smart hosts, etc. Refer to your Exchange administrator.

Create a journal rule

Add a journal rule as follows:

- Journal outbound email to <your journal address>

To create a new journal rule:

1. Open Exchange PowerShell (also known as the Exchange Management Shell.
2. Enter the following command:

```
new-journalrule -journalemailaddress
journal@worksharedetectserver.local -name "Detect Server" -Scope
External -Enable $true
```

***Note**: You can limit journaling to a specific set of senders.*

Create a receive connector

Add a receive connector for administrators and users to receive user management emails and custom reports.

To create a receive connector:

1. Open Exchange PowerShell (also known as the Exchange Management Shell.

2. Enter the following command:

```
$receiveConnector = new-ReceiveConnector -Name:'Workshare Detect
Receive Connector' `-Usage:'Custom' `-Bindings:'0.0.0.0:25' `-
RemoteIPRanges:$RemoteIpRange `-AuthMechanism:
'ExternalAuthoritative' `-PermissionGroups:'ExchangeServers'
`-MaxMessageSize $MaxMessageSize -Enabled $Enabled -ErrorVariable
$err
```

***Note**: The above is an example. Everything with a $ in its name is a variable that needs to be changed.*

(optional) Step 6: Custom property stamping on documents

Detect Server uses custom properties within email attachments to identify documents and understand policy violation. These custom properties can be inserted manually, using template macros, or using a server-side tool. With manual and template macros, end-user training is required; with the server-side tool, no end-user workflows are affected.

A recommended server-side tool is the Worksmart DLPTagger tool from HBR Consulting for iManage installations. This tool is installed either co-located on the iManage server, or on a separate machine. The DLPTagger tool watches for save or re-index operations, and then tags documents within workspaces of interest with a pre-configured set of workspace properties.

The steps for installing the Worksmart DLPTagger tool are explained in detail in the DLPTagger Admin Guide. The prerequisites for the tool are:

- **Software:**
  - Operating system: Windows 7 or above
  - iManage: Version 8.5 or above
- **Access prerequisites:**
  - The DLPTagger service needs read access to the iManage DB catalog, and write access to its own DB catalog
  - The installation requires an Administrator-level (on the machine) service account that the DLPTagger service will run as. This service account needs to be able to access the iManage DB catalog (read-only) and the DLPTagger DB catalog (read-write)

(optional) Step 7: Business intelligence reporting

Detect Server reports anomalies and perceived risk scores using a reporting layer. Starting in version 1.6, one report has been included as part of Detect Server. Over future releases, all the reports enabled by Detect Server will be included.

Until all reports are included, Detect Server still requires a standalone off the shelf reporting system. Workshare has created and configured reports using Tableau. A full-scale commercial installation will require a Tableau Server installation along with Tableau Desktop instances. All Tableau software will be licensed separately and directly from Tableau Software.

The Tableau installation is fed directly from the SQL Server storing all the aggregated data produced by Detect Server. It would be possible to present this information on an in-house business intelligence (BI) system. In this scenario, Workshare's Professional Services team will work with your in-house BI team to set up reports on your BI system.

Chapter 3: Configuration

This chapter describes how to configure settings for Workshare Detect Server in the Settings area of the console. It includes the following sections:

- **Domain Classification**, page 35, describes how to classify email domains in order to run queries against a particular email domain.
- **Selecting Emails to Monitor**, page 36, describes how to configure Detect Server to process only the email of selected senders.
- **Inviting Users**, page 39, describes how to provide other users with access to the Detect Server console.

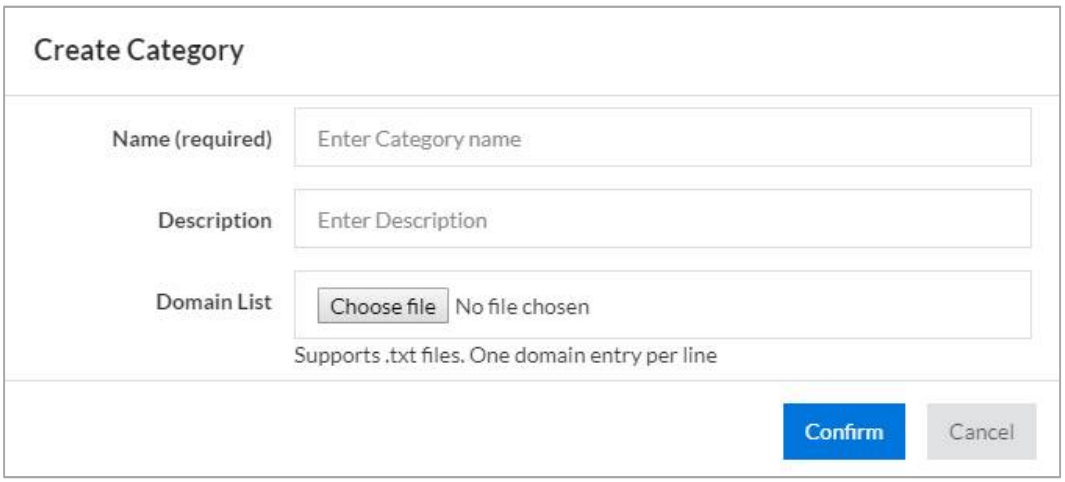
Domain Classification

You identify and classify email domains in order to run queries against a particular email domain. For example, classify a group of domains as “Newspapers/Press” or another as “Competitors”. Reporting of email activity to these domains requires bespoke configuration on Tableau Server, which involves professional services.

There are three default domain categories set up in Detect Server – Non-corporate domains, Internal domains and Restricted domains. This should enable you to start monitoring immediately but if you want to create additional domains, the procedure is below.

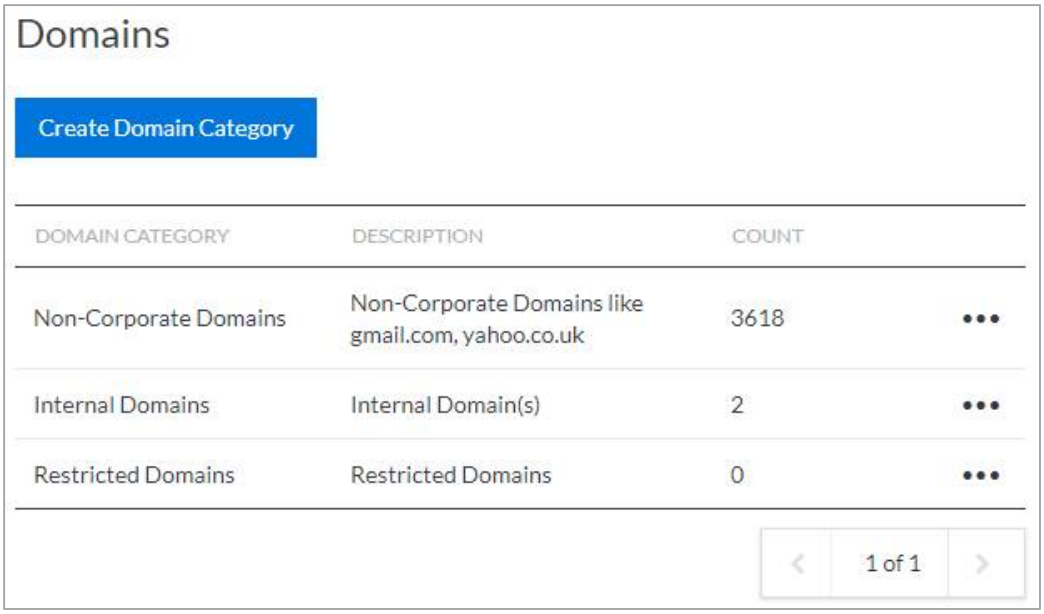
To classify domains:

1. First of all, create a text file listing the domains you want to monitor. You can enter multiple domains, but each must be on a separate line. You can also download a list of domains from a blacklisting services site.
2. In the Workshare Detect Server console, click the Settings icon and then select the **Domains** tab.
3. Click **Create Domain Category**.



4. Add a name for your new domain list and a suitable description.
5. Click **Choose file** and browse to your saved text file.

6. Click **Confirm**.



You can now select this domain category when creating a report.

***Note**: You can use the options in the ••• menu to the right of the domain category to edit or delete it, or to download the text file.*

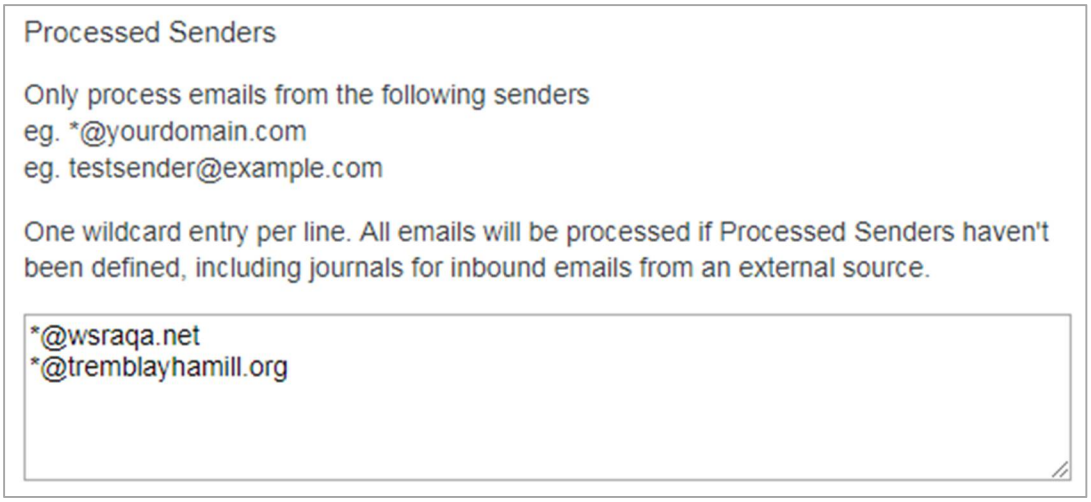
Selecting Emails to Monitor

By default, Detect Server processes journals (copies) of all outbound email sent externally. You can configure Detect Server to process only the email from selected senders.

To select emails:

1. In the Detect Server console, click the Settings icon and then select the **Email processing** tab.

2. Scroll to the **Processed Senders** area.



3. Enter the domains you want to monitor. By default, Detect Server processes all emails if nothing is specified here. You can specify a whole domain, such as *@workshare.com or just a couple of users on that domain. When entering multiple domains, put each on a separate line.
4. Click **Save Changes**.

Protect Server configuration

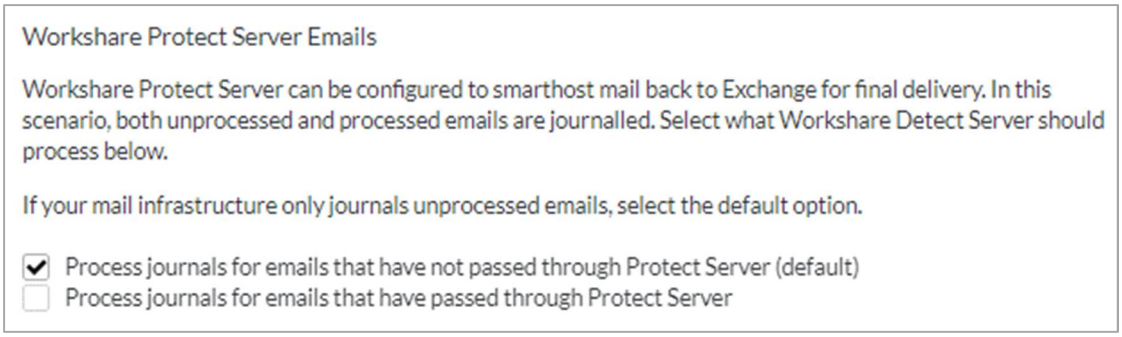
When you have Workshare Protect Server and the Workshare Protect Routing Agent set up in your email environment, a journal is made of emails going into Protect Server and again when they come out, before they are sent on for final delivery. You can select whether you want Detect Server to process both these journals or just one. By default, Detect Server processes journals of emails made before the email is processed by Protect Server.

***Note**: This is only when you're working with Protect Server AND the Routing Agent.*

To configure processing with Protect Server:

1. In the Detect Server console, click the Settings icon and then select the **Email processing** tab.

2. Scroll to the **Workshare Protect Server Emails** area.



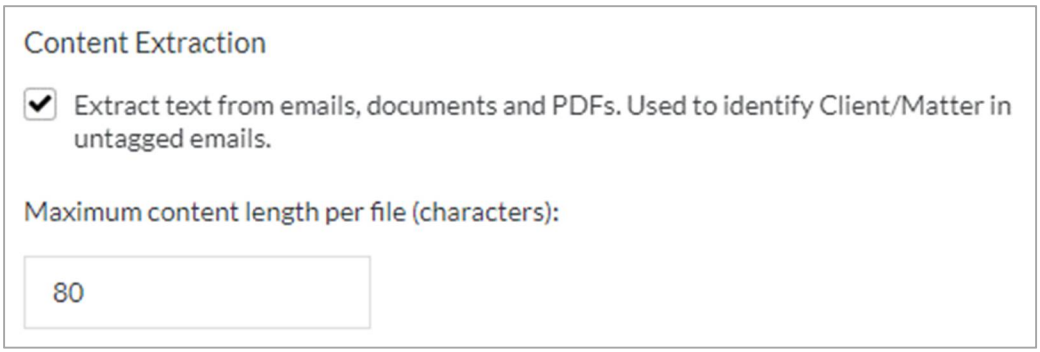
3. Select either or both of the checkboxes.
   - **Process journals for emails that have not passed through Protect Server**: Detect Server processes journals (copies) of emails made before the email is processed by Protect Server.
   - **Process journals for emails that have passed through Protect Server**: Detect Server processes journals (copies) of emails made after the email has been processed by Protect Server.
4. Click **Save Changes**.

Content extraction

You can configure Detect Server to pull content from the body of the attachment to get more information about the document. This could help to identify the matter ID or the type of document being sent.

To enable content extraction:

1. In the Detect Server console, click the Settings icon and then select the **Email processing** tab.
2. Scroll to the **Content Extraction** area.



3. Select the checkbox and click **Save Changes**.

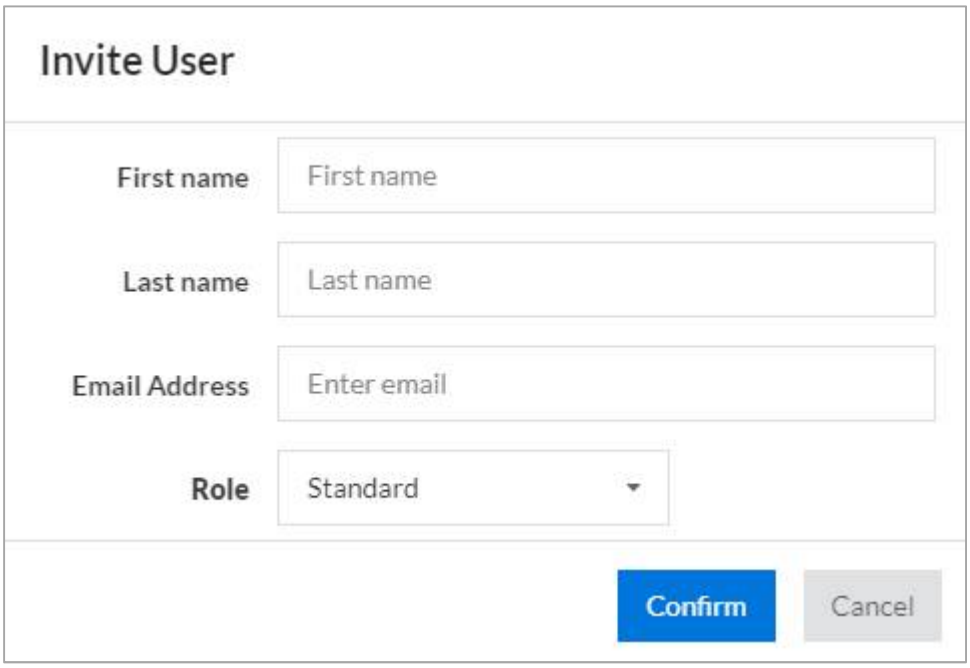
Inviting Users

The first person that logs in to Workshare Detect Server becomes an administrator user. The administrator user can then invite other users to Detect Server and can assign them a user or administrator role.

- Users with an **Administrator** role can access all areas of the Detect Server console so they can run reports, monitor the status of the Detect Server system and configure settings. They can also invite other users to Detect Server.
- Users with a **User** role can run reports. They cannot access the configuration via the Settings icon .

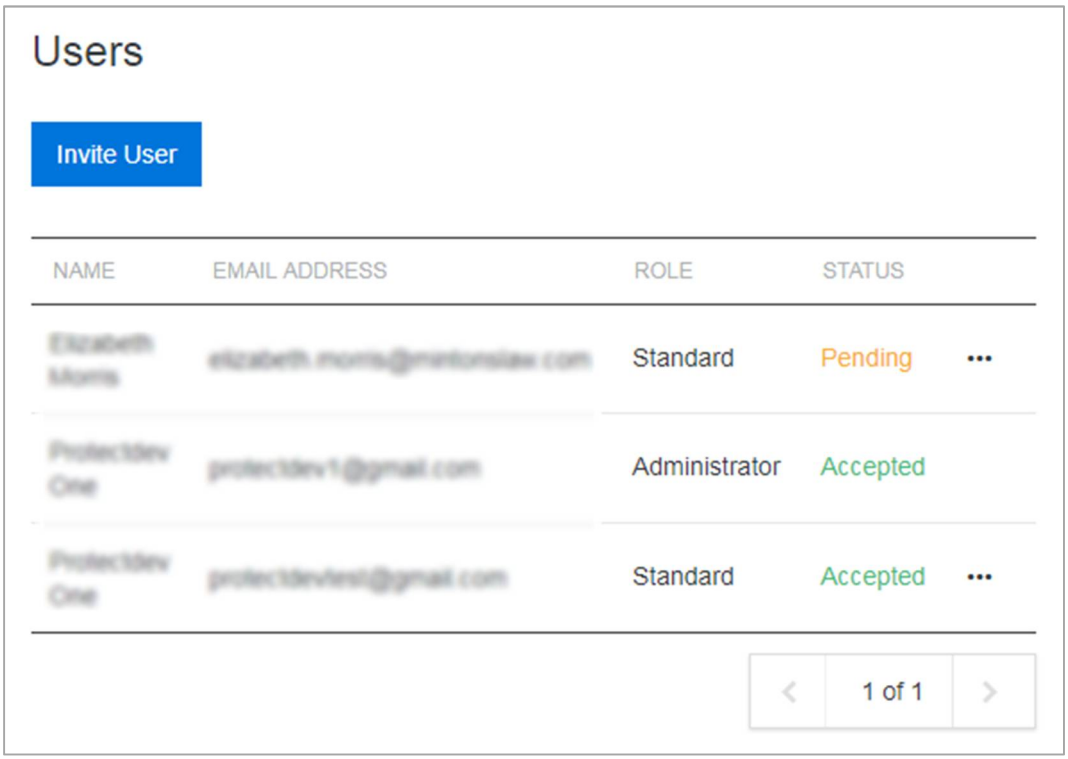
To invite people to Detect Server:

1. Log into the Detect Server console, click the Settings icon and then select the **Users** tab.
2. Click **Invite User**.



3. Enter the name and email address of the person you want to invite to Detect Server.
4. Select whether you want the invited user to have a **Standard** or **Administrator** role.

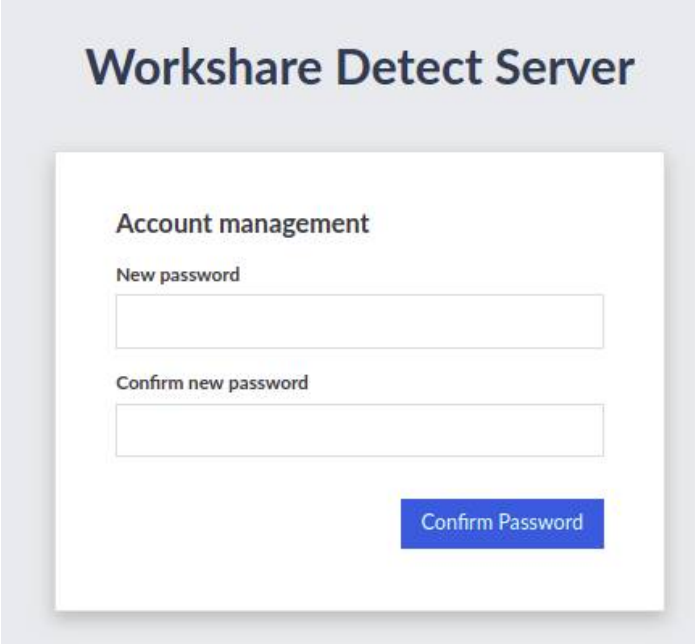
5. Click **Confirm**. An invitation is sent to the email address inviting the recipient to join Detect Server. Until the recipient accepts, you will see them in the user list with the status “Pending”.



Tip! *You can delete a user or change their role at any time using the options in the ••• menu to the right of the user.*

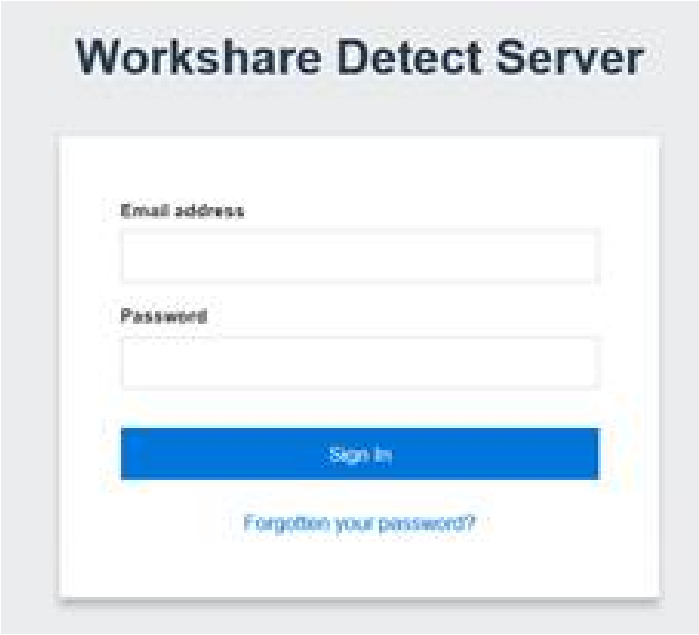
What the invited user sees

The invited user will receive an email with a link to join Detect Server. Once they click the link, they are prompted to create a login password.



They must enter a password twice and click **Confirm Password**.

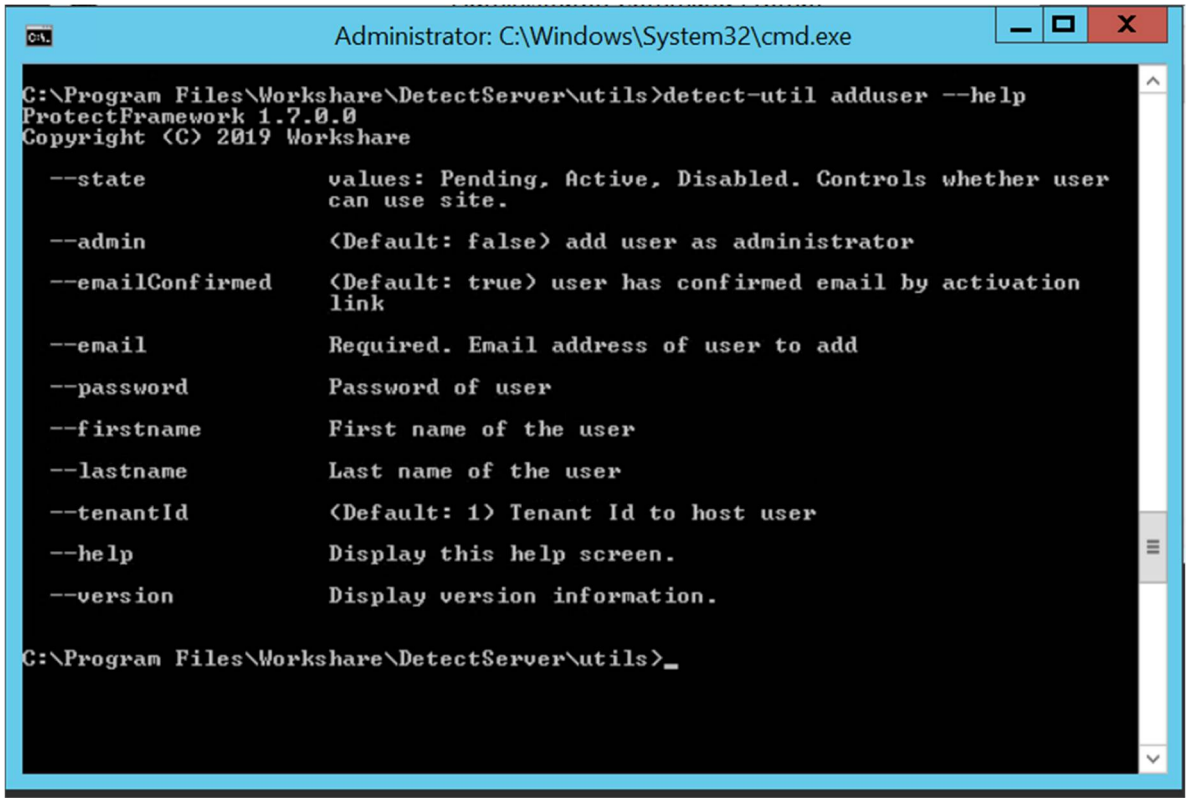
Then the user can click **Go to login page** in the Success message and log in to Detect Server using their email address and password.



Command utility to add users

Alternatively, you can use a command line utility to add a user and set a password. Then you must send the user a link to Detect Server and details of the password you have set for them.

To add users using the command line, follow the example below:



Revisions
Published for Workshare Detect Server 1.7: 12/04/19

Workshare Ltd., 20 Fashion Street, London E1 6PX www.workshare.com