Enterprise Connect Passwordless Server Installation Guide

Version 6.8

Table of Contents

Enterprise Connect Passwordless Server Installation: Overview

This document provides step-by-step installation instructions to establish an Enterprise Connect Passwordless environment.

The Authentication Server is typically deployed on the enterprise domain, where it is configured to access the directory service and to work with relying parties that are either on-premise or off. Connecting to the directory service allows the administrator to assign authenticators to users and define authentication policies. Connecting with the relying parties can be done by configuring standard interfaces (e.g., RADIUS, SAML, etc.) or by defining a non-standard interface.

In some cases, the Authentication Server authenticates the user and produces the required attestation for the relying party. In other situations, the Authentication Server may need to also facilitate the exchange of a session secret required by the relying party. For example, legacy systems that are still heavily password dependent may require that a password be produced. In such cases, the Authentication Server provides a temporary session password that is reset at the end of the session.

The administrator configures the system settings from the Enterprise Connect Passwordless Management Console.

Installation Options

When you run the Enterprise Connect Passwordless Authentication Server installation package, you will be prompted to choose one of four installation options:

```
Please select one of the installation options:
  1. Management Console
  2. Authentication Server
  3. Authentication Server in the DMZ
  4. All-in-One (complete solution on a single server)
```

Important

The All-in-One installation option should be used for POC environments only.

For production deployments, the best practice is to install the **Management Console** and **Authentication Server** separately. The database may be created as part of the Management Console Server installation, or it can be configured later by the administrator as a necessary first step of the Management Console configuration.

Installation of an **Authentication Server in the DMZ** may be required in configurations where users are required to authenticate to services while outside the enterprise's network without using a VPN connection. In this installation option, the system will include two or more Authentication Servers inside your network and at least one server in the DMZ.

For larger scale deployments, we recommend that each component be installed on a separate server. In addition, the installation of the distributed architecture should have at least two servers from each component, to support high availability in case of failure of one of the components.

POC Deployments

The All-in-One option is the recommended mode of installation for **POC environments only**. This option installs the Management Console, an Authentication Server and a database in a single installation process.

To improve availability and redundancy of Enterprise Connect Passwordless Authentication and to increase performance, the system supports balancing by adding additional Authentication Servers to the system. Following All-in-One installation, you can install a second Authentication Server on a different machine, and then configure the communication protocols.

When required, an Authentication Server in the DMZ may be added to POC deployments. The DMZ Server must be connected to an additional Authentication Server that is installed separately (NOT the Authentication Server installed as part of the All-in-One setup).

Installation of a secondary Management Console Server is not supported in POC environments.

Installation Prerequisites

During installation, the installation script creates a user named *SDO* for running its services. If an existing SDO user is found, the script will spontaneously abort.

In order to ensure that the script can run as expected,
do NOT manually create a user named SDO prior to installation and verify that there is no element in your environment (group, folder, etc.) named *SDO*.

Before beginning the installation process, make sure that you have:

- Linux base OS (64-bit) with Minimal image option - Red Hat 8.2 to 8.10 / Red Hat 9.3 to 9.5, Oracle Linux 8.3 to 8.10 / Oracle Linux 9.3 to 9.5, or Rocky Linux 8.4 to 8.10 / Rocky Linux 9.3 - 9.5.

Important

If you are using Linux 9 and the tar command is not pre-installed on your machine, please run the following command **before** installing Enterprise Connect Passwordless Authentication Server:

yum install tar

Authentication Server version 6.8 does not support Linux 7 (el7). In addition, Red Hat versions 8.0 and 8.1 and CentOS (all versions) are no longer supported. Attempts to install the Enterprise Connect Passwordless authentication solution on these versions will be automatically aborted.

Important

The Enterprise Connect Passwordless solution can be installed on Red Hat 9.x, but it may **NOT** be upgraded to 9.x from a system already installed on Red Hat 8.x using the usual upgrade methods. If you need to upgrade ALL solution components to version 9.x, refer to System Upgrade to Red Hat 9.x.

- Authentication Server's FQDN and Public IP

- Authentication Server installation file (**enterprise-connect-passwordless- el8/el9-<build number>.run**)
- Authentication Server activation file and its password

  Checksum (.md5), Authentication Server activation file (.LIC) and a corresponding Code will be provided by the support team as required.
- Corporate's root-CA or Self-signed CA (to establish Nginx secure connection)
- Corporate's Mail Server details (SMTP)
- **For Active Directory Passwordless authentication only:** The Domain controller or root CA is required. The domain controller should be signed by the domain CA.

Note

The Checksum MD5 file is provided to verify the integrity of the installation file. To run the validation check, use the syntax in the following example, with the name of the relevant installation file.

md5sum -c enterprise-connect-passwordless-el8-6.8.run.md5

Minimum Hardware Requirements

Verify that the following minimum requirements are met:

System Component	Cores	RAM	Disk Space	Notes
Management Console Server	4x cores	16GB	100GB	
Authentication Server	4x cores	8GB	50GB	Up to 2,000 concurrent authentications
Authentication Server DMZ	2x cores	8GB	50GB	Up to 2,000 concurrent authentications
All-in-One Server for POC	2x cores	10GB	40GB	This hardware should only be used for POC only

Required Configurations

Required firewall policy configurations are listed in the table below.

Source	Destination	Port	Description
Management Console Server	User (LDAP) Directory Server	TCP - LDAP/S 389/636	User LDAP Directory synchronization
Management Console Server	Mail (SMTP) Server	TCP – SMTP/S 25/587/465	Mail Server communication
RADIUS Client	Authentication Server	UDP - RADIUS 1812/1813/7351/1645/1646	RADIUS authentication
Authentication Server	Cloud Web Services	TCP - HTTPS 443	According to the connection: HTTP/ HTTPS
Windows / Mac workstations	Authentication Server	TCP - HTTPS 443	Windows AD authentication
Admin Terminal	Authentication Server	TCP - HTTP/S 8008/8443	Administrator access to the Management Console
Authentication Server	Management Console	TCP 2222	Tunnel from the Authentication Server to the Management Console (configurable during the installation)
Authentication Server DMZ	Authentication Server	TCP 22	Tunnel from the Authentication Server DMZ to the internal Authentication Server
Management Console	Enterprise DB Server	DB Server Port	Connection from the MC to the Enterprise DB Server

The load balancer should be configured as termination or forwarding. The host name should be the same for both external and internal load balancers (resolve the same DNS name from external and internal).

Required Ports

The following table lists all ports that the Authentication Server requires for normal operation. These ports need to be available for successful installation and system operation.

Port Number	Applicable Role	Service	Notes
443	AIO/AUTH/DMZ	nginx	portal/rest/adpa
2222	MC/AIO	sdomcbe/sshd	default/user configurable
4444	MC/AIO	sdomcbe	auth → mc comm
5555	AIO/AUTH/DMZ	reverse proxy (nginx) for the portal (local)	
5432	MC/AIO	postgresql	if configured and running
6379	MC/AIO/AUTH	redis	
9600/10000	MC/AIO	logstash	
8008	MC/AIO	nginx	/api and /doc when ssl is disabled
8080	AIO/AUTH/DMZ	reverse proxy (nginx) for webauthn (local)	
8443	MC/AIO	nginx	/api and /doc when ssl is enabled
3000	MC/AIO	reverse proxy (nginx) for sdomcbe	/api and /doc on 8443 or 8008
3331	AIO/AUTH/DMZ	reverse proxy (nginx) for sdomon/rest (local)	mc → auth comm
3332	AIO/AUTH/DMZ	reverse proxy (nginx) for sdomon/adpa	
3333	AIO/AUTH/DMZ	reverse proxy (nginx) for sdomon/rest	
3334	AIO/AUTH/DMZ	reverse proxy (nginx) for sdomon/saml	

3340	AIO/AUTH/DMZ	reverse proxy (nginx) for sdomon/saml (metadata)	
9200/9300	AIO/MC	elasticsearch	
13700 + slot_id	MC/AIO	sdotun	mc → auth comm. Allocated for each connected authserver. The slot_id can be found in /opt/sdo/.conf of the authserver.
14444	AIO/AUTH/DMZ	sdotun	auth → mc comm tunneling
16379	AUTH/DMZ/secondaryMC	sdotun	redis tunneling
10001	AUTH/DMZ/AIO	sdotun	logstash tunneling
12000 + dir_id	AUTH/AIO	ldap-proxy	

Supported Databases

The following database types and versions are supported:

Database Type	Minimum Version	Maximum Version
PostgreSQL	PostgreSQL 9	PostgreSQL 15
MS SQL	SQL Server 2012 SP4	SQL Server 2022
Oracle	Oracle Database 12c	Oracle Database 19c

For more information about database requirements, refer to Appendix C: Database Configuration.

Supported Browsers

Browser	Supported Versions
Chrome	30 and higher

Safari	13.1.2 and higher
Firefox	25 and higher
Edge	41 and higher

Enterprise Connect Passwordless Management Console Server Installation

This installation option is intended to install only the Enterprise Connect Passwordless Management Console and database (if needed). Following installation, there is a stand-alone Management Console, without an Authentication Server.

For the system to work properly, you will need to install an Authentication Server installed on a separate server. The Authentication Server can be installed only after the Management Console installation is completed.

Important

Before beginning the installation process, review the list of prerequisites.

Follow the procedure below to install the Management Console Server.

To perform Management Console Server installation:

1. Run the Authentication Server installation package:

   ```
   sudo ./enterprise-connect-passwordless-####.run
   ```

2. To choose the Management Console installation option, enter **1**.

   ```
   Please select one of the installation options:
     1. Management Console
     2. Authentication Server
     3. Authentication Server in the DMZ
     4. All-in-One (complete solution on a single server)

   Select an option: 1
   ```

3. Specify the setting for installing as a secondary Management Console (default = no).

   ```
   Install as a secondary Management Console (y/N)? n
   ```

   If you are installing a secondary Management Console, type **y** and follow the procedure for Secondary Server Installation.

4. When prompted, enter the port number to be used for the SSH connection between the Management Console and the Authentication Server.

   ```
   Enter a port number that will be used for inter-server communication:
     port: 2222
   ```

5. Specify the setting for firewall creation (default = yes).

```
Do you want the installer to configure the firewall (Y/n)? y
```

To skip firewall creation, type **n**. It will then be necessary to ensure that the Linux firewall is configured correctly, according to the chosen configuration:

- **With SSL:** Ports 443 and 8443 are enabled
- **Without SSL:** Ports 80, 8008 and 8009 are enabled accordingly

6. Select a database configuration setting (default = yes).

```
Do you want to use a local PostgreSQL DB (Y/n)? y
```

If you don't want to use a local PostgreSQL database, type **n**. Manual configuration of a database will then be your *first* step when you log into the Management Console for the first time.

Important

If you choose to use a local (internal) PostgreSQL database, keep in mind that you will NOT be able to migrate it to an external database later on.

7. Enter Administrator login details for the Management Console.

```
Enter administrator login details for the Management Console:
  Email: admin@domain.com
  Password (must be at least 8 characters in length):
  Retype password:
```

Delete the default email setting and enter the correct email address. Then enter and retype the password.

8. Enter details for the self-signed certificate:

- **Organization Name:** Delete *My Org* and enter the correct name.
- **Server Name:** Enter the server name for the certificate. (The name will appear as known on the Linux server. Change it if necessary.)

```
Processing certificates...
  Creating new certificate(s), enter certificate details:
    Organization Name: ACME Corp
    Server Name: octopusauth
done
```

9. Verify that the installation completed successfully.

```
Enter administrator login details for the Management Console:
  Email: admin@abc.com
  Password (must be at least 8 characters in length):
  Retype password:

Processing certificates...

  Creating new certificate(s), enter certificate details:
    Organization Name: My Org
    Server Name: octopusauth

Finalizing... done

Enable/Start nginx... done
Enable/Start services... done
Waiting for MCBE... ready
Initialize db... done

Installation Successful

[root@localhost amitl]#
```

10. To enable the new GUI to be uploaded, perform a hard refresh to the browser, or clear the browser cache.

To complete setup of the Management Console, log into the Management Console, activate Enterprise Connect Passwordless Authentication and configure the SMTP communication of the system. For details, refer to Management Console: Basic Configuration.

Important

If you did not use a local PostgreSQL database, manual configuration of a database needs to be your first step after logging into the Management Console. For details, refer to Appendix C: Database Configuration.

Secondary Management Console Server Installation

This installation option installs a stand-alone Management Console without an Authentication Server. It is intended to provide a standby (ready to run) Enterprise Connect Passwordless Management Console.

The secondary (standby) Management Console is not an active component of the distribution but it continuously runs in the background and is synchronized with the primary Management Console. It can therefore be quickly changed to act as the primary Management Console when necessary.

Important

Secondary Management Console (MC) Server installation can be done only in a distributed installation, where the secondary MC Server communicates with and uses the installed database.

A secondary MC Server cannot be installed for All-in-One (AIO) installations, since the database is internal on the AIO machine.

After reviewing the list of prerequisites, follow the procedure below to install a secondary Management Console Server.

Important

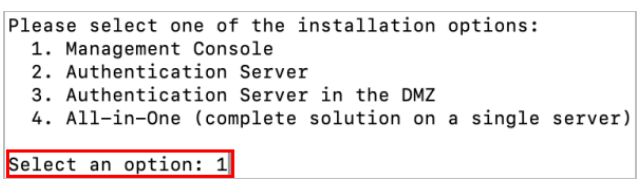
Before beginning the installation, make sure that the primary Management Console is installed **and configured**. For details, refer to Management Console: Basic Configuration.

To install a secondary Management Console Server:

1. Run the Authentication Server installation package:

   ```
   sudo ./enterprise-connect-passwordless-####.run
   ```

2. To choose the Management Console installation option, enter **1**.

3. Specify the setting for installing as a secondary Management Console:

```
Install as a secondary Management Console (y/N)? n
```

Change the default setting by typing **y** .

4. When prompted, enter the port number to be used for the SSH connection between the Management Console and the Authentication Server.

```
Enter a port number that will be used for inter-server communication:
  port: 2222
```

5. Specify the setting for firewall creation (default = yes).

```
Do you want the installer to configure the firewall (Y/n)? y
```

To skip firewall creation, type **n**. It will then be necessary to ensure that the Linux firewall is configured correctly, according to the chosen configuration:

   - **With SSL:** Ports 443 and 8443 are enabled
   - **Without SSL:** Ports 80, 8008 and 8009 are enabled accordingly

6. Enter Administrator login details for the Management Console.

```
Enter administrator login details for the Management Console:
  Email: admin@domain.com
  Password (must be at least 8 characters in length):
  Retype password:
```

Delete the default email setting and enter the correct email address. Then enter and retype the password.

7. Enter details for the self-signed certificate:

   - **Organization Name:** Delete *My Org* and enter the correct name.
   - **Server Name:** Enter the server name for the certificate. (The name will appear as known on the Linux server. Change it if necessary.)

```
Processing certificates...
  Creating new certificate(s), enter certificate details:
    Organization Name: ACME Corp
    Server Name: octopusauth
done
```

8. Manual create an SSH trust on the primary Management Console, using the public key that is generated by the installation:

```
Setting primary Management Console trust...

Manually create an ssh trust on the primary Management Console, use this public key:

ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDRFEBIKc4qp1+ErQoC5z/Nhvuf02H+9XSUOVLGFCDZesv3Q
PWDo02KQawe9TU5bG5nxuTXkLLSVNHhOagvFyJmvVfbWj8JYoWD+8smEM2G6mbck2sD7ynnG9baXc0ORGhDwo
A0/cCoAaqfPC/VhAEr74Fn9fvl+2mXAGuWcrdjg+jjyPJQ2Crh4IytIamIaePi3dMJOclwQ8rSoYgUzVi6Ool
LxuG4X4ewsLOSqPNdSJQ+ObygcamBiRg0csQaQLl6FVcqQNJYUKe3ja4Fh4DNV sdo@cqa4.com


Please enter the address of the primary Management Console
Make sure it is running and accessable stand-alone installation
  address:
```

   a. In the **primary** Management Console Server, move to the 'Superuser' shell:

```
sudo bash
```

b. Change user to sdo:

```
su – sdo
```

c. Change directory to .ssh:

```
cd /opt/sdo/.ssh/
```

d. Open an editor to edit / create a file:

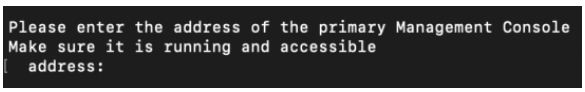
```
vi authorized_keys
```

e. Copy the public key from the secondary Management Console Server, and paste it into the **primary** Management Console Server. Save and then exit editing mode.

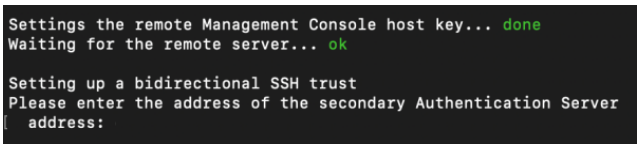
f. Change permissions to remove group write permissions:

```
chmod g-w authorized_keys
```

9. In the secondary Management Console Server, enter the IP address or FQDN of the primary Management Console Server.



10. When prompted, enter the address of the secondary MC Server, as seen from the primary MC Server. (This creates a bidirectional SSH trust, which allows syncing between the servers when the primary MC Server is toggled to become secondary.)



11. Verify that the installation completed successfully.

12. To enable the new GUI to be uploaded, perform a hard refresh to the browser, or clean the browser cache.

Switching Between Primary and Secondary Management Consoles

Follow these steps to change the secondary Management Console to the main one:

1. On the primary Management Console, run the *toggle_mc.sh*:

```
cd /opt/sdo/scripts
sudo toggle_mc.sh
```

2. Update the DNS record of the Management Console to reflect the IP switch (from primary to secondary).

3. On the secondary Management Console, run the *toggle_mc.sh*:

```
cd /opt/sdo/scripts
sudo toggle_mc.sh
systemctl restart nginx
```

Authentication Server Installation

Installation of Enterprise Connect Passwordless Authentication Servers is done as part of a distributed deployment and/or to provide additional servers for high availability. Authentication Server installation may be required in either of the following configuration options:

- For deployment to a production environment, you need to install a Management Console Server and an Authentication Server as **separate servers**.

  In this case, install the Management Console server **first**. Make sure that server is up and running and before installing the Authentication Server. Once both servers are installed, configure them to function as one system.

- **All-in-One additional Authentication Server:** To improve availability and redundancy of authentication and to increase performance in a POC environment, Enterprise Connect Passwordless Authentication enables load balancing by adding additional Authentication Servers.

  Before beginning installation of the additional Authentication Server, verify that the All-in-One Server is up and running.

Follow the procedure below to install an Authentication Server.

To install an Authentication Server:

1. Run the Authentication Server installation package:

   ```
   sudo ./enterprise-connect-passwordless-####.run
   ```

2. To choose the Authentication Server installation option, enter **2**.

   ```
   Please select one of the installation options:
     1. Management Console
     2. Authentication Server
     3. Authentication Server in the DMZ
     4. All-in-One (complete solution on a single server)

   Select an option: 2
   ```

3. When prompted, enter the port number to be used for the SSH connection between the Management Console and the Authentication Server.

   ```
   Enter a port number that will be used for inter-server communication:
     port: 2222
   ```

4. Specify the setting for proxy configuration (default = no).

```
Do you want to use a proxy for HTTPS access to the Octopus Cloud Server (y/N)? n
```

For network setups in which HTTPS to the internet is accessed through a proxy server, type **y** and enter the URL or IP address of your proxy server.

5. Specify the setting for firewall creation (default = yes).

```
Do you want the installer to configure the firewall (Y/n)? y
```

To skip firewall creation, type **n**. It will then be necessary to ensure that the Linux firewall is configured correctly, according to the chosen configuration:

   - **With SSL:** Ports 443 and 8443 are enabled
   - **Without SSL:** Ports 80, 8008 and 8009 are enabled accordingly

6. Enter details for the self-signed certificate:

   - **Organization Name:** Delete *My Org* and enter the correct name.
   - **Server Name:** Enter the server name for the certificate. (The name will appear as known on the Linux server. Change it if necessary.)

```
Processing certificates...
  Creating new certificate(s), enter certificate details:
    Organization Name: ACME Corp
    Server Name: octopusauth
done
```

7. Enter a name for the Authentication Server. This name will be used to identify the server within the Management Console.

   After you enter a name, the setup will generate a Configuration String. This is the server's Public Key that you will copy and paste to the Management Console in the next step.

```
Please enter a name for the Authentication Server, it will be
used to identify the server within the Octopus Management Console
  name: acme.com

Please copy the configuration string below into the Octopus Management Console:

ewogICAgIm5hbWUiIDogImFjbWUuY29tIiwKICAgICJwdWJsaWNLZXkiIDogInNzaC1yc2EgQUFBQUIzTnphQzF5YzJFQUFBQURBUU
TkdMUU43czV4bkRIR1B4R1dQOGNXdnJyMlZ6QmJpRm96NHRPSWdIWUpFZTlseUZJS1ZHWndvVWkxbldISzBZQ3V6SGw2UmxZY0sraU
UERTdWM1eWduZUx2T2t5V1R4IHNkb0BjZW50b3M3NWF1dGgucWFzZG8uY29tIiwKICAgICJpZCIgOiAiZDYwOGZkOTYtNzFjNC00Nj
```

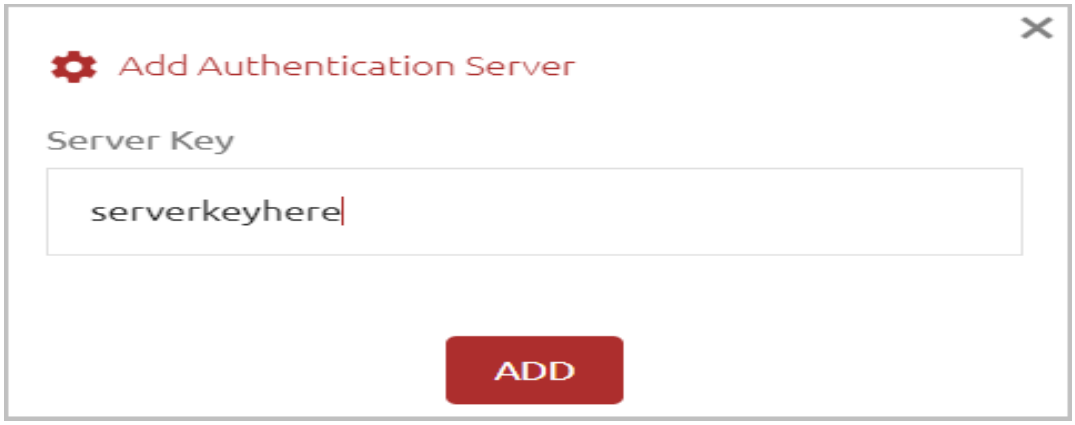
8. Add the Authentication Server to the Management Console:

   a. In the Management Console, navigate to **System Settings > Auth Servers**.

   b. At the top of the page, click **Add Server**.

      The **Add Authentication Server** popup opens.

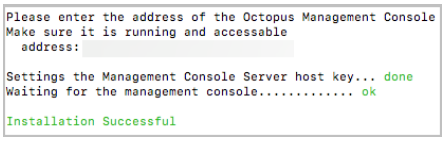
   c. Paste the server key in the field, and then click **Add**.



The Authentication Server is added to the Management Console.

9. Return to the Authentication Server SSH screen, and type the address of the Management Console. Be sure to use the complete domain name (FQDN) of the Management Console, *not* the IP address.

10. Verify that the installation completed successfully.



Authentication Server in the DMZ Installation

Installation of an Authentication Server in the DMZ may be required in configurations where users need authentication to services while outside the enterprise's network and there is a preference not to use a VPN connection.

An Authentication Server in the DMZ may only be installed and added to a system that already has at least one Authentication Server running. Due to security considerations, the Authentication Server in the DMZ does not have its own database. It must be connected to a system that already has an Authentication Server and database.

Important

A DMZ Server connects directly to ONE (and only one) corresponding internal Authentication Server via an SSH tunnel. Do NOT use a load balancer to connect a DMZ Server with its Authentication Server.

Installation Flow for POC Environments

In POC environments, the DMZ Server must be connected to an additional Authentication Server that has been installed separately (**not** the Authentication Server set up in the All-in-One installation). To add a DMZ Server to an All-in-One installation environment, do the following:

1. Install an additional Authentication Server.

2. Install the Authentication Server in the DMZ, and connect it to the new Authentication Server, as described in the following sections.

Preparing for Installation

Before beginning the installation, take the following steps:

1. Review the list of prerequisites.
2. Open two SSH terminal connections in parallel:
    - DMZ Authentication Server terminal window
    - Authentication Server terminal window
3. In the DMZ Authentication Server, go to the home directory.

Installing an Authentication Server in the DMZ

Follow the procedure below to install an Authentication Server in the DMZ.

To install an Authentication Server in the DMZ:

1. Run the Authentication Server installation package:

    ```
    sudo ./enterprise-connect-passwordless-####.run
    ```

2. To choose the Authentication Server in the DMZ installation option, enter **3**.

    ```
    Please select one of the installation options:
      1. Management Console
      2. Authentication Server
      3. Authentication Server in the DMZ
      4. All-in-One (complete solution on a single server)

    Select an option: 3
    ```

3. Specify the setting for proxy configuration (default = no).

    ```
    Do you want to use a proxy for HTTPS access to the Octopus Cloud Server (y/N)? n
    ```

    For network setups in which HTTPS to the internet is accessed through a proxy server, type **y** and enter the URL or IP address of your proxy server.

4. Specify the setting for firewall creation (default = yes).

    ```
    Do you want the installer to configure the firewall (Y/n)? y
    ```

    To skip firewall creation, type **n**. It will then be necessary to ensure that the Linux firewall is configured correctly, according to the chosen configuration:

    - **With SSL:** Ports 443 and 8443 are enabled
    - **Without SSL:** Ports 80, 8008 and 8009 are enabled accordingly

5. Enter details for the self-signed certificate:
    - **Organization Name:** Delete *My Org* and enter the correct name.

- **Server Name:** Enter the server name for the certificate. (The name will appear as known on the Linux server. Change it if necessary.)

```
Processing certificates...
  Creating new certificate(s), enter certificate details:
    Organization Name: ACME Corp
    Server Name: octopusauth
done
```

6. Manually create an SSH trust on the Authentication Server, using the public key that is generated by the installation:

```
Manually create an ssh trust on the adjacent authenticator, use this public key:

ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQC5itquhWdBCTeixJNVJoPA8LmXAvAKI+3WumVh5dBd/NpF7ycSyxG09Ol1nDH30Y2rBYIV8h/
bDg8JQ+yhX4E4Ptx7XE/vQ95iX3YggeEkWH6wW9dgutxSgMy7b2BNyp/9PyrV7QSmuUPPR6oLTmuy49ZFA65zD6oJz3nx/9Hz5NJa22py5C/ s
```

   a. In the Authentication Server, move to the 'Superuser' shell:

      ```
      sudo bash
      ```

   b. Change user to sdo:

      ```
      su – sdo
      ```

   c. Change directory to .ssh:

      ```
      cd /opt/sdo/.ssh/
      ```

   d. Open an editor to edit / create a file:

      ```
      vi authorized_keys
      ```

   e. Copy the public key from the DMZ Server, and paste it into the Authentication Server. Save and then exit editing mode.

   f. Change permissions to remove group write permissions:

      ```
      chmod g-w authorized_keys
      ```

7. Verify that there is communication between the DMZ Server and the Authentication Server.

8. Verify that the installation completed successfully.

```
Please enter the address of the Remote Authentication Server
Make sure it is running and accessable
  address: 10.0.4.119

Settings the Remote Authentication Server host key... done
Waiting for the remote server... ok

Installation Successful
```

Authentication Server All-in-One Installation

The following sections provide step-by-step instructions for the All-in-One installation option. This installation includes the Management Console, Authentication Server and Database.

Important

The All-in-One installation option should be used for POC environments only.

Following All-in-One installation, you can install one or more additional Authentication Servers to improve availability and redundancy of Enterprise Connect Passwordless authentication and to increase performance. Authentication Servers in the DMZ are also supported for POC deployments. Make sure that the DMZ Server is connected to an additional Authentication Server (NOT the Authentication Server installed as part of the All-in-One setup).

Installation of a secondary Management Console Server is not supported in POC environments.

Before beginning the All-in-One installation process, review the list of prerequisites.

Preparing for All-in-One Installation

Perform the following steps to set up your POC environment:

1. Open an SSH connection to the machine you are going to install on.
2. Go to the home directory and run the following command:

   ```
   sudo cd
   ```

3. Modify the installation package's permissions by running the following command:

   ```
   sudo chmod +x enterprise-connect-passwordless-####.run
   ```

Performing All-in-One Installation

Follow the procedure below to perform All-in-One installation.

To perform All-in-One installation:

1. Run the Authentication Server installation package:

   ```
   sudo ./enterprise-connect-passwordless-####.run
   ```

2. To choose the All-in-One installation option, enter **4**.

   ```
   Please select one of the installation options:
     1. Management Console
     2. Authentication Server
     3. Authentication Server in the DMZ
     4. All-in-One (complete solution on a single server)

   Select an option: 4
   ```

3. When prompted, enter the port number to be used for the SSH connection between the Management Console and the Authentication Server.

   ```
   Installing RPMs... done

   Enter a port number that will be used for inter-server communication:
     port: 2222
   ```

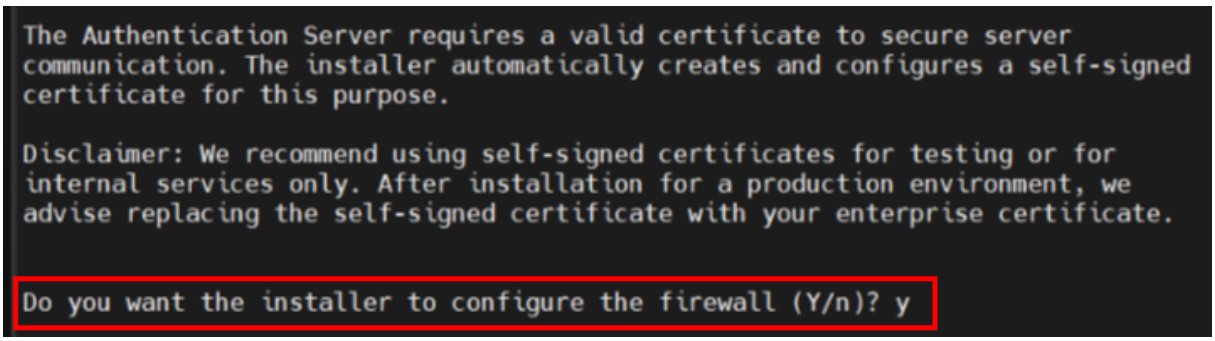
4. Specify the setting for proxy configuration (default = no).

For network setups in which a proxy server connects to the Internet, type **y** and then enter the URL or IP address of your proxy server.

Note

This setting can also be configured post-installation.

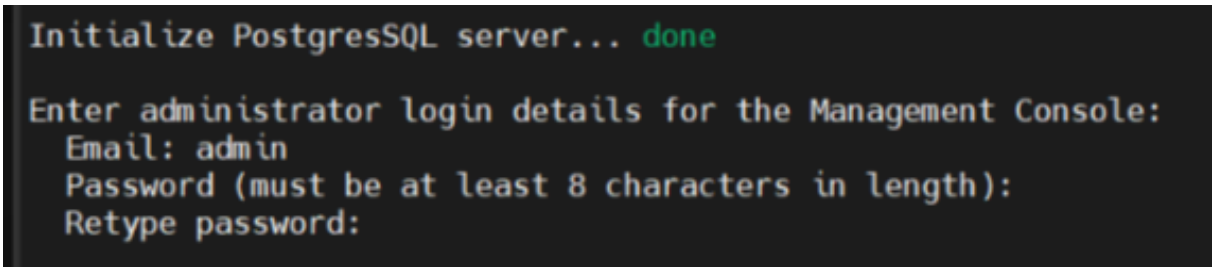
5. Specify the setting for firewall creation (default = yes).



To skip firewall creation, type **n**. It will then be necessary to ensure that the Linux firewall is configured correctly, according to the chosen configuration:

- **With SSL:** Ports 443 and 8443 are enabled
- **Without SSL:** Ports 80, 8008 and 8009 are enabled accordingly

6. Enter Administrator login details for the Management Console.



Delete the default email setting and enter the correct email address. Then enter and retype the password.

7. Enter details for the self-signed certificate:

- **Organization Name:** Delete *My Org* and enter the correct name.
- **Server Name:** Enter the server name for the certificate. (The name will appear as known on the Linux server. Change it if necessary.)

```
Processing certificates...
  Creating new certificate(s), enter certificate details:
    Organization Name: My Org
    Server Name: rh88m[redacted].com
done
```

8. Verify that the installation completed successfully.

```
  sdomcbe.service... ok
  sdomon.service... ok
  sdoportal.service... ok
  sdorproc.service... ok
  sdorsched.service... ok
  sdoservice-ldap.service... ok
  sdotun.service... ok
  sdoweba.service... ok
  sdocleanup.timer... ok
  elasticsearch.service... ok
  logstash.service... ok
done


Adjusting ElasticSearch (data stream)...
  Waiting for MCBE... ready
done

Initialize db... done

Configure local db with the MCBE... done
Setting local Authentication Server connection... done
Update Redis db1... done

Installation Successful
```

Post-installation Steps

Before continuing, consider performing the Authentication Server Sanity Check. We recommend doing the sanity check if you suspect something went wrong during setup, or to confirm that you performed all required tests. For details about the sanity check, refer to Appendix A.

To complete setup of the All-in-One Authentication Server, log into the Management Console, activate Enterprise Connect Passwordless authentication and configure the SMTP communication of the system. For details, refer to Management Console: Basic Configuration.

Authentication Server Upgrade

Upgrade is supported for Authentication Servers and Management Console servers. Upgrade of an All-in-One environment is **NOT** supported.

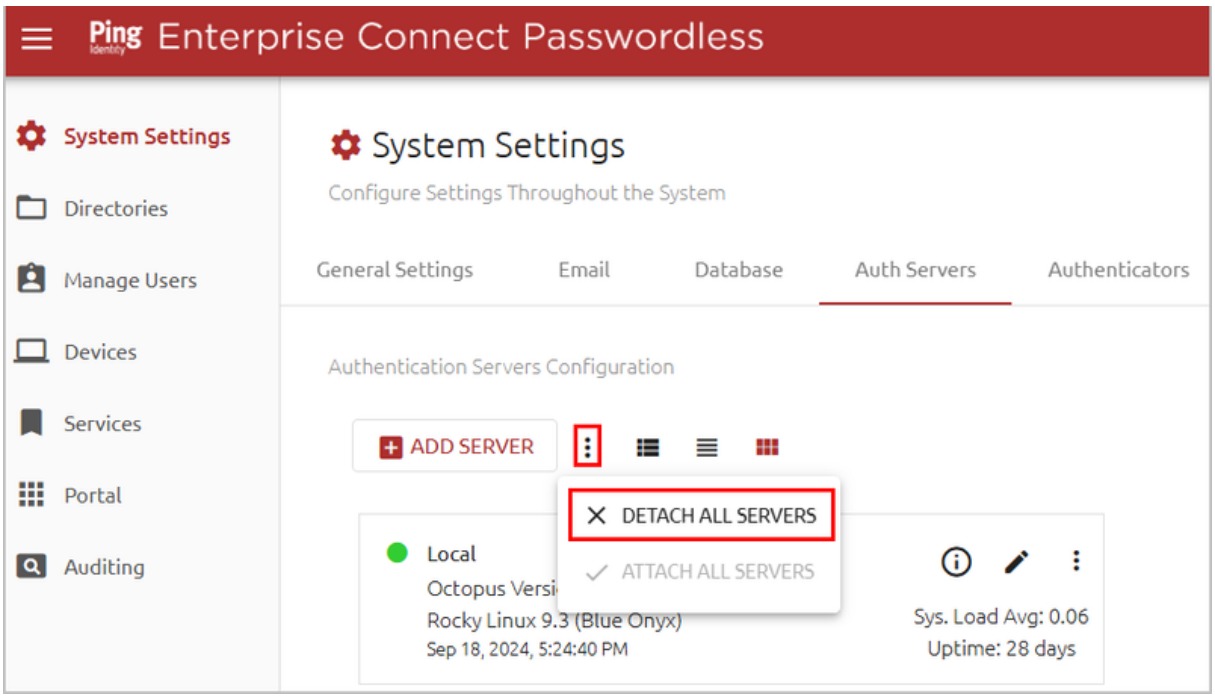
In distributed server configurations, it is recommended to follow the steps described in the sections below. These upgrade processes perform a full backup of the current system, ensuring no loss of data or settings.

Important

If your environment includes a DMZ Server, upgrade it after performing the distributed server upgrade described in the following procedure. For instructions about DMZ upgrade, refer to Upgrading DMZ Servers.

To perform upgrade for distributed servers:

1. From the Management Console (**System Settings > Auth Servers**), detach the Authentication Server from the Management Console. If you have more than one Authentication Server, detach all of them.

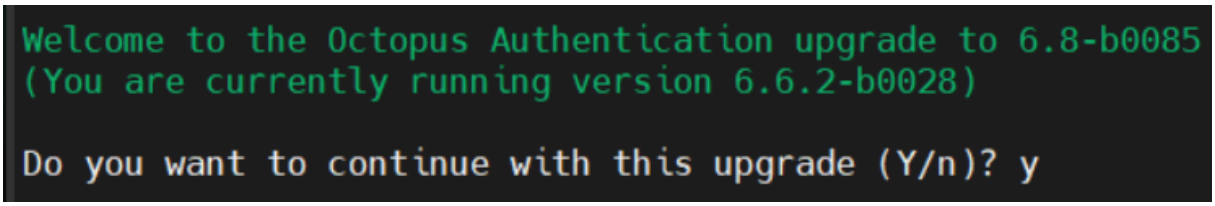


   After you detach the servers, they will continue to authenticate users, and the Management Console will be ready for upgrade.

2. Run the Management Console upgrade by executing the Authentication Server upgrade script:

   ```
   sudo ./enterprise-connect-passwordless-####.run
   ```

   The installation will display the currently running version and prompt you to confirm that you want to proceed with the upgrade.



3. Specify the setting for firewall configuration (default = yes).

4. Verify that the installation completed successfully.

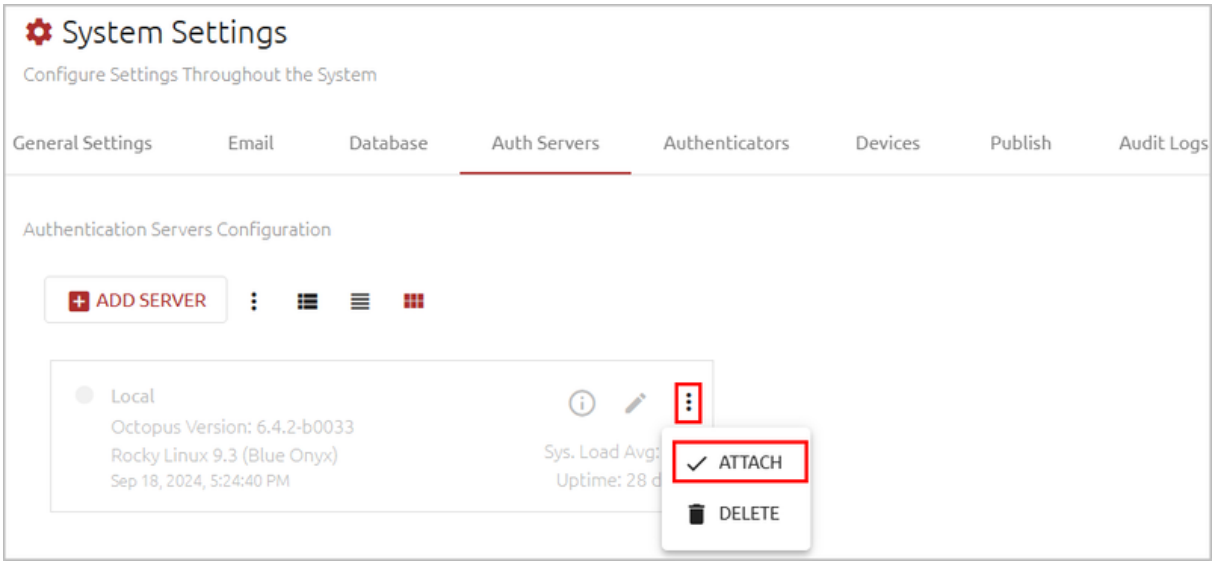
```
Do you want to continue with this upgrade (Y/n)? y

Migrating ElasticSearch (index)... done
Installing RPMs... done
Installing SELinux module... done
Update Redis configuration... done
Enable/Start Redis... done

Do you want the installer to configure the firewall (Y/n)? y

Processing certificates... done

Enable/Start nginx... done
Migrating db schema... done
Enable/Start services... done
Adjusting ElasticSearch (data stream)... done
Waiting for MCBE... ready
Refresh Redis db0... done
Update Redis db1... done

Installation Successful
```

5. If you have a Secondary Management Console (MC), upgrade it by executing the Authentication Server upgrade script, as described in Steps 2-4 above.

   If you do not have a Secondary MC, continue with Step 6.

6. Disconnect the first Authentication Server from the load balancer. Run the upgrade script on the server, and verify that the installation completed successfully.

7. From the Management Console (**System Settings > Auth Servers**), attach the Authentication Server back to the MC.



8. Connect the first Authentication Server back to the load balancer.
9. Repeat Steps 6-8 for all additional Authentication Servers.
10. When the upgrade process is complete, restart the server.
11. To enable the new Management Console GUI and the User Portal interface to be uploaded, perform a hard refresh to the browser (**Ctrl + F5**), or clear the browser cache.

    Note that a license warning ("Error reading license") will appear in the MC until the first Authentication Server is reattached. If you continue to see this error, verify that all Authentication Servers are reconnected. The connection process may take several minutes.

Note

After upgrade, if you need to change the port number for the SSH connection between the Management Console and the Authentication Server, run the following script: *change_tun_port.sh*

This script is located in the **/opt/sdo/scripts** folder.

Upgrading DMZ Servers

If your configuration includes a DMZ Server, follow the procedure below to upgrade this server.

Important

The DMZ Server upgrade should be done **after** completing the distributed server upgrade described above.

There is no need to detach servers from the Management Console before performing DMZ Server upgrade.

When upgrading to version 6.8, there is no need to rename the certificate file after completing the upgrade. The name of your file will be maintained automatically during the upgrade process.

To upgrade a DMZ Server:

1. Remove the public key from the DMZ Server that was used to create an SSH trust on the Authentication Server:
    a. In the Authentication Server, move to the 'Superuser' shell:

    ```
    sudo bash
    ```

    b. Change user to sdo:

    ```
    su – sdo
    ```

    c. Change directory to .ssh:

    ```
    cd /opt/sdo/.ssh/
    ```

    d. Open an editor to edit / create a file:

    ```
    vi authorized_keys
    ```

e. Remove the public key from the Authentication Server. Save and then exit editing mode.

f. Change permissions to remove group write permissions:

```
chmod g-w authorized_keys
```

2. Run the upgrade by executing the Authentication Server upgrade script:

```
sudo ./enterprise-connect-passwordless-####.run
```

3. To obtain the public key for the DMZ server, execute the (*update_remote*) script:

4. Manually create an SSH trust on the Authentication Server, using the public key generated:

a. In the Authentication Server, move to the 'Superuser' shell, change user to sdo, change directory to .ssh, and open an editor. (For details, see commands **a-d** in Step 1 above.)

b. Copy the public key from the DMZ Server, and paste it into the Authentication Server. Save and then exit editing mode.

c. Change permissions to remove group write permissions:

```
chmod g-w authorized_keys
```

5. Verify that there is communication between the DMZ Server and the Authentication Server.

6. Verify that the installation completed successfully.

Note

After upgrade, if you need to change the port number for the SSH connection between the Management Console and the Authentication Server, run the following script: *change_tun_port.sh*

This script is located in the **/opt/sdo/scripts** folder.

Management Console: Basic Configuration

The following sections describe the configurations that are required for basic setup of the Management Console:

- Configuring General Settings: Entering the Enterprise Base URL, specifying organization name and logo, and setting various global parameters related to authentication sessions
- Configuring Mail Server Settings: Setting SMTP server information and other required email parameters
- Adding Directories: Integrating the Management Console with one or more directories

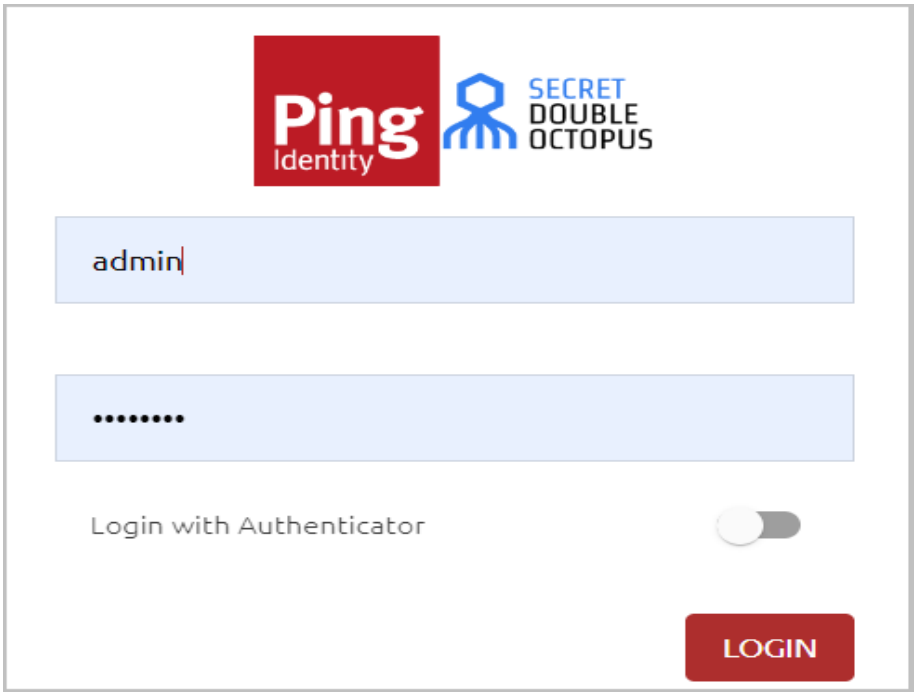
To log into the Management Console:

1. From your desktop browser, launch the Management Console. (e.g., *https://myorg.com:8443* or *http://myorg.com:8008*).

> **Note**
>
> For HTTPS secure connection (SSL/TLS), you will need to enforce an SSL certificate (RootCA, IntermediateCA or Self-Signed CA) for the Nginx engine (Red Hat Linux Web Server).

   The Login screen opens.

2. Make sure that the **Login with Authenticator** toggle button is inactive. Then, enter the username and password set during the installation, and click **LOGIN**.



   Following successful authentication, the Management Console opens.

Configuring General Settings

Basic system configurations that need to be done following installation include setting the Enterprise Base URL, specifying the organization name and logo, and setting global parameters related to authentication sessions.

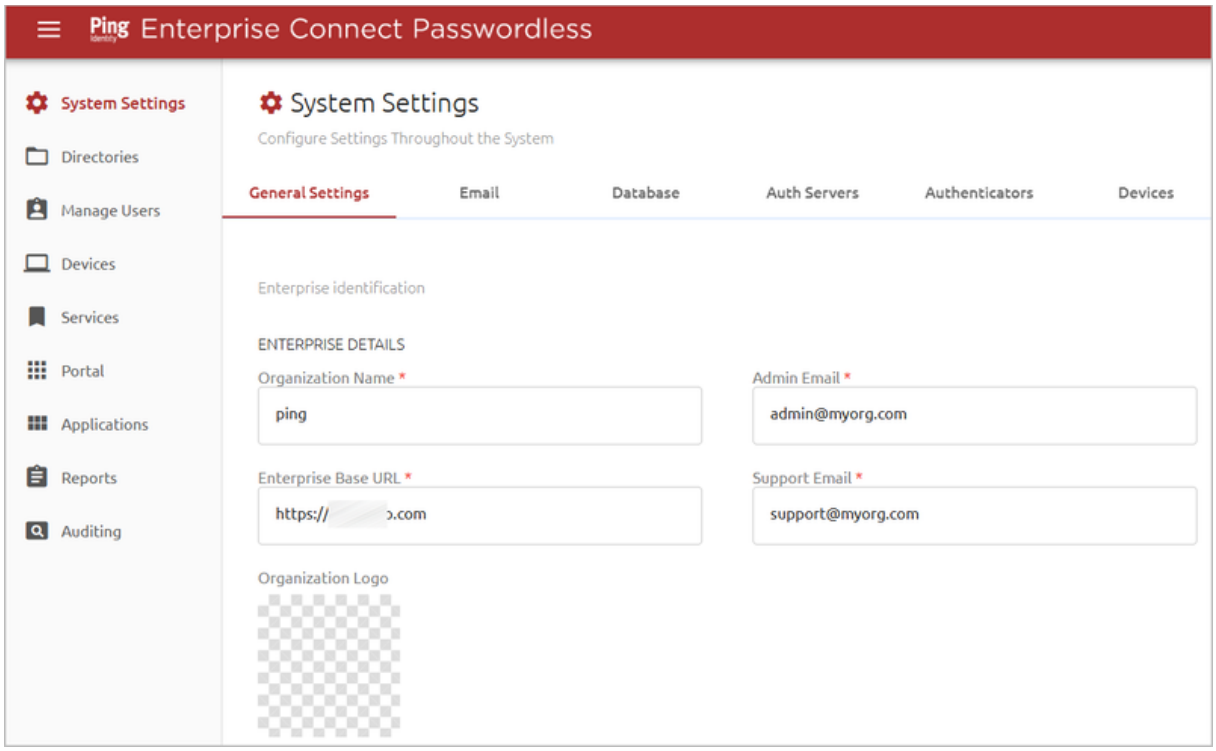
These settings are configured in the **General Settings** tab of the **System Settings** menu.

Setting Organization Name, Enterprise Base URL and Logo

The organization name and logo you set in the Management Console are displayed to users in the Authenticator mobile app. The default **Organization Name** is the one entered during installation of the Authentication Server. You may change the name, as necessary.

The **Organization Logo** setting is empty by default. To upload a logo, hover over the area, click **Upload File** and select the PNG or JPG file of your choice. Supported image size is 128x128 pixels.

Your **Enterprise Base URL** is the URL of the main server used for communications.



After updating the settings, click **Save** (at the bottom of the tab).

Setting Authenticator Limit and MC Session Timeout

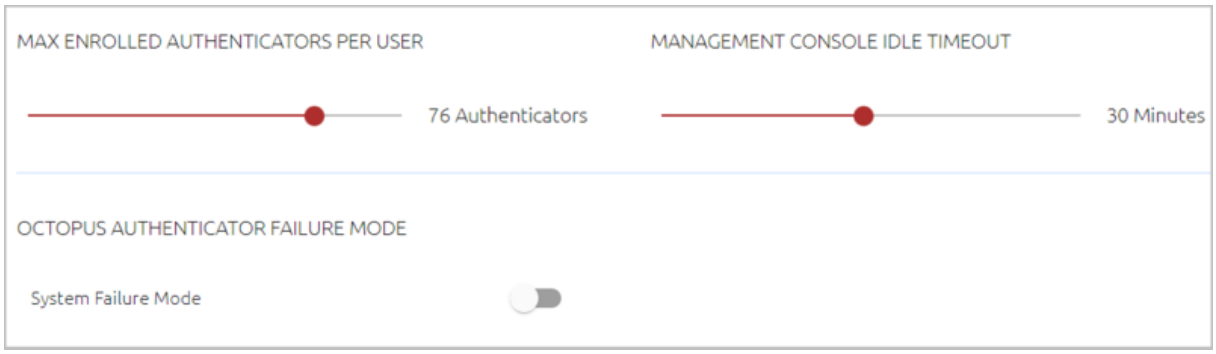
The lower portion of the **General Settings** tab contains various settings related to authentication sessions.

The settings are:

- **Max Enrolled Authenticators Per User:** The maximum number of authentication devices that can be enrolled in the system for each user. Valid values can range from 1-99. Drag the slider to adjust the value.
- **Management Console Idle Timeout:** The length of time (in minutes) during which no actions are performed in the Management Console before the session is automatically ended. Values can range from 1-60 (default is 10).

  Octopus Authenticator Failure Mode: This setting determines the behavior of the system in situations of network failure or unavailability of the Authentication

Server. When System Failure Mode is enabled, authentication for all services is done with a username and password in the event of system failure.

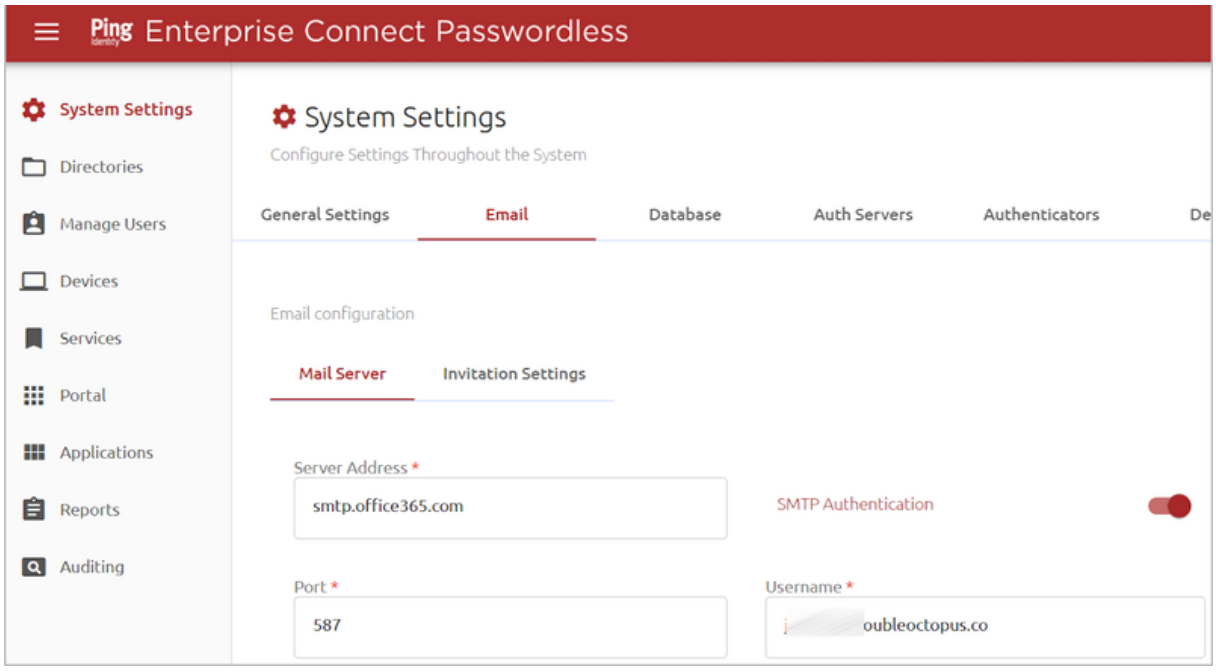


After updating these settings, click **Save**.

Configuring Mail Server Settings

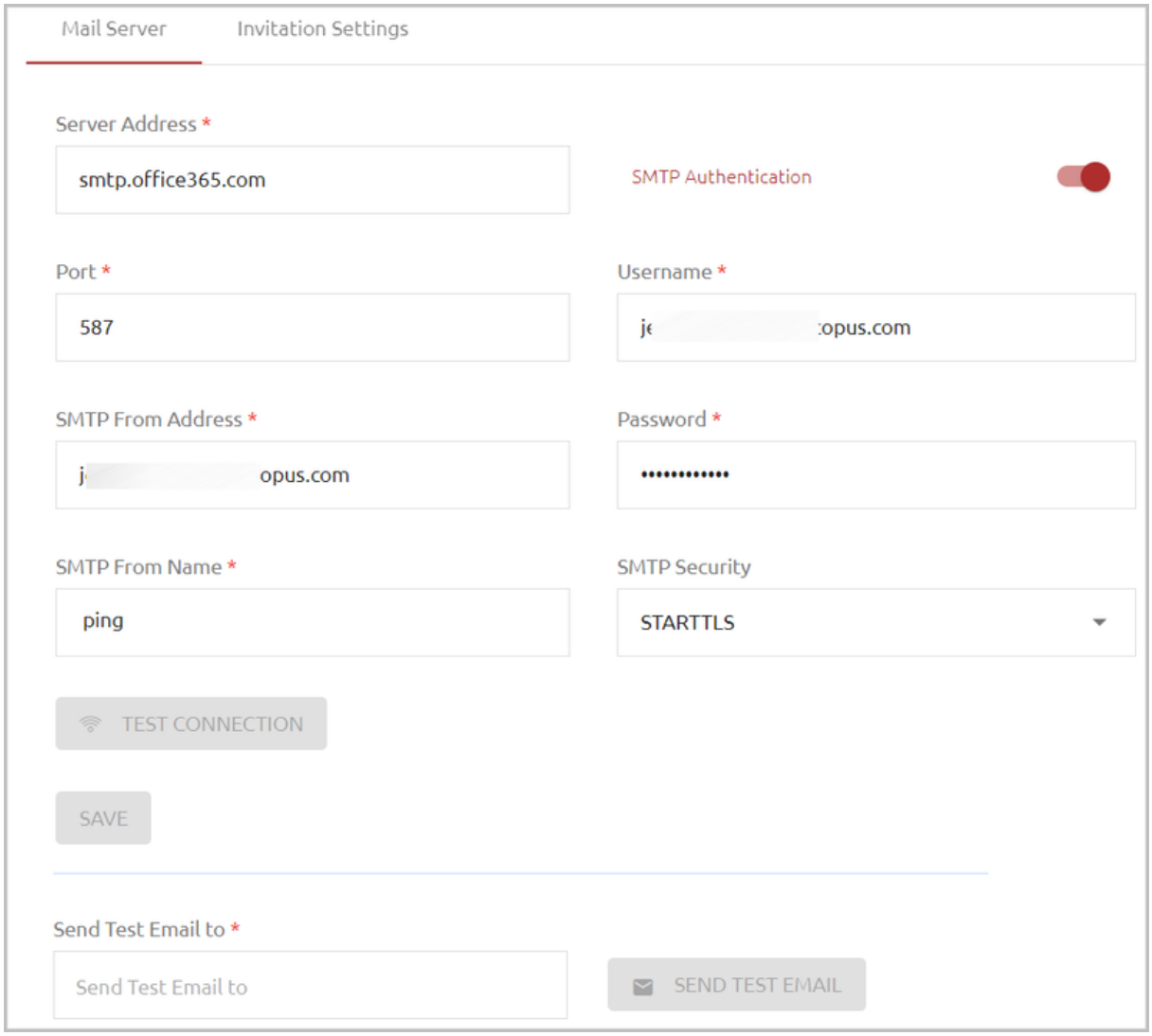
SMTP configuration is required to allow system administrators to send emails inviting users to enroll in the Enterprise Connect Passwordless solution. It is also necessary to enable system alert notification emails to the administrator.

To view the configuration settings, open the **System Settings** menu and select the **Email** tab.



Configuring Server Details

The **Mail Server** sub-tab contains SMTP server information and other required email parameters.



To set up SMTP server details:

1. Enter the following parameters in the appropriate fields:
    - **Server Address:** IP address or hostname of the SMTP server
    - **Port:** Port number for SMTP connection
    - **SMTP From Address:** The From email address that appears in system-generated emails
    - **SMTP From Name:** The name of the sender that appears in system-generated emails
2. Select the appropriate **SMTP Security** method: SSL/TLS or STARTTLS
3. If you want to use SMTP authentication, click the toggle button at the upper right corner of the tab (by default authentication is inactivated), and enter the authentication username and password.
4. Click **Test Connection**.

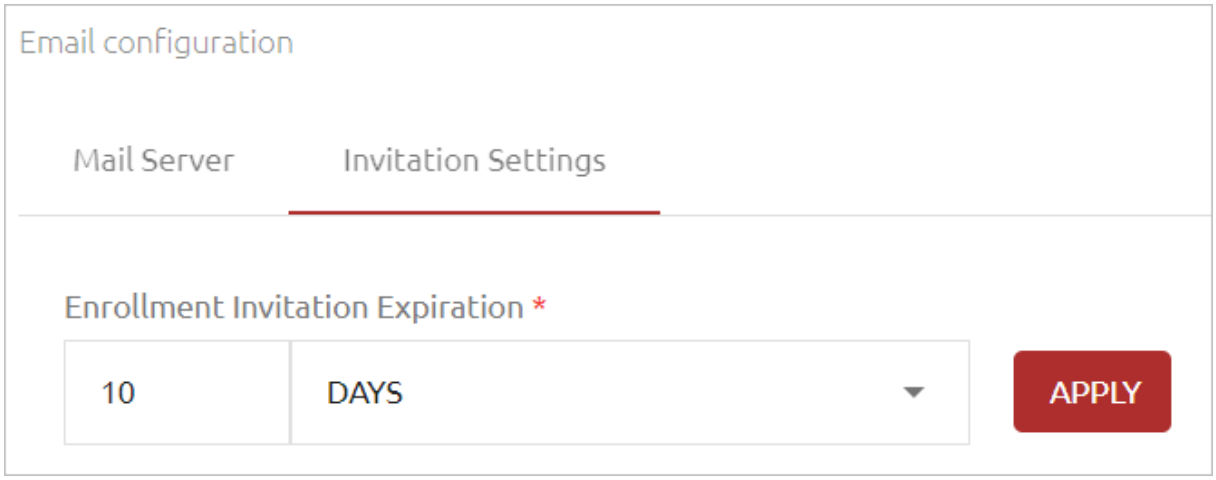
Following the test, a confirmation message is displayed at the bottom of the page.

5. Click **Save**. Then, from the toolbar at the top of the page, click **PUBLISH** and publish your changes.
6. To verify expected performance, enter a valid email address in the **Send Test Email To** field and click **Send Test Email**. Then, check that an email message was sent and received correctly.

Setting Enrollment Token Expiration

The **Invitation Settings** sub-tab contains the **Enrollment Invitation Expiration** setting, which determines the maximum period of time for which an invitation email is valid. If a user does not use the invitation to enroll within this time period, the invitation is deleted from the system and a new email needs to be sent.

The **Enrollment Invitation Expiration** can range from 1 hour to 3 weeks (default setting is 3 days). To update the value, specify the desired timeframe and then click **Apply**.



Adding Directories

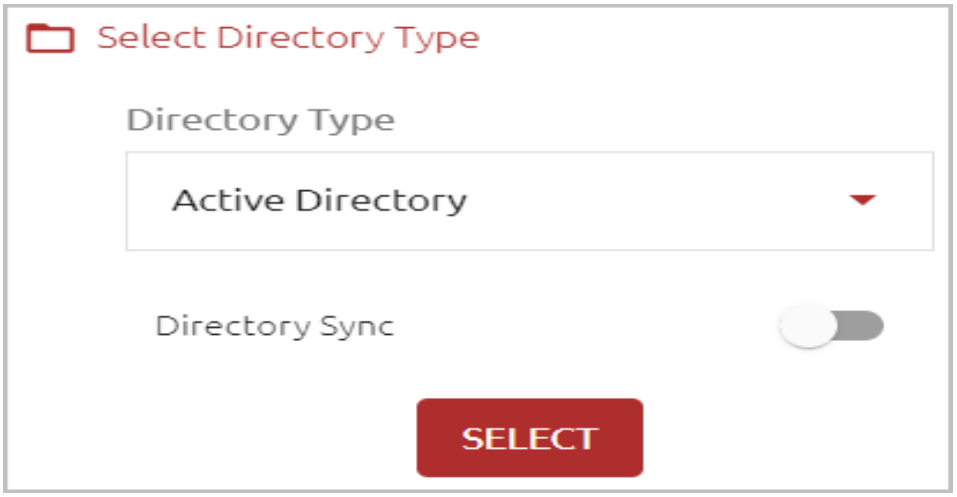
The Management Console supports integration with multiple directory types, including Active Directory, Entra ID, ForgeRock, ForgeRock Cloud, Oracle/Open LDAP and Google. You can configure integration with more than one directory type.

The following procedure explains how to integrate AD, ForgeRock and ForgeRock Cloud directories. For information about other directory types, refer to the Enterprise Connect Passwordless Management Console Admin Guide.

To add a new directory:

1. Open the **Directories** menu and click **Create Directory**.

   The **Select Directory Type** dialog opens.



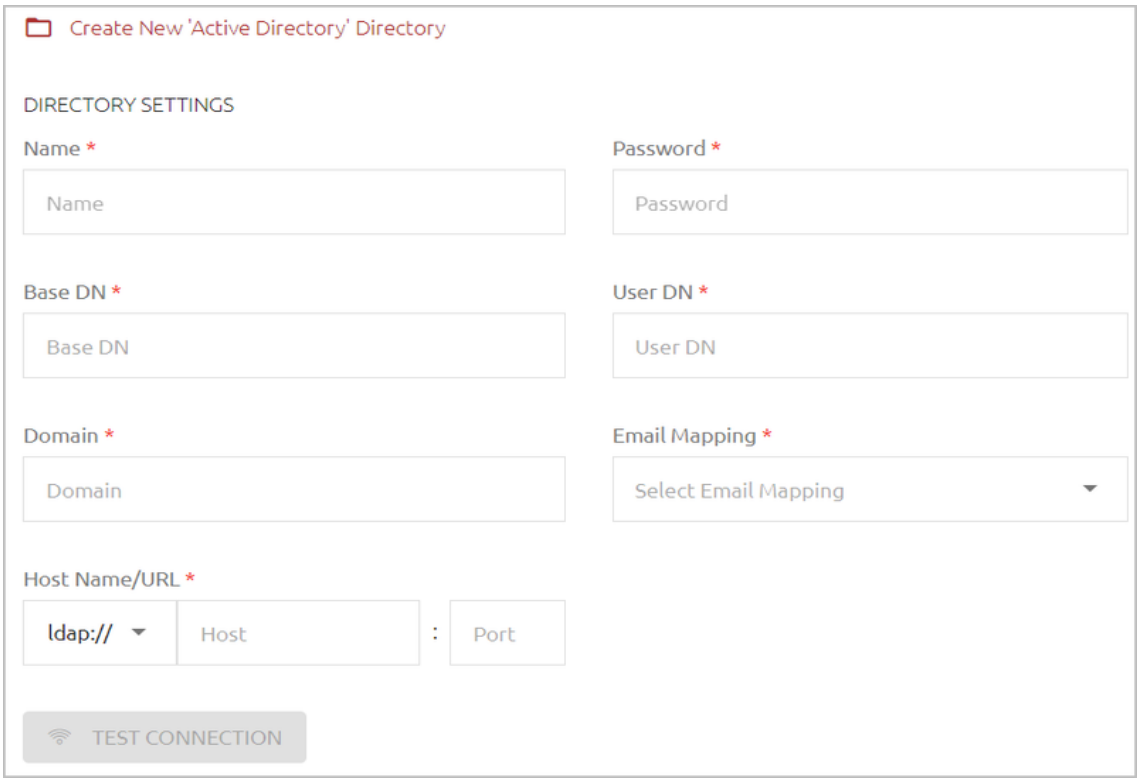
2. From the **Directory Type** list, select the type of directory that you want to add.
3. Click the **Directory Sync** toggle button to enable and disable automatic syncing. When automatic directory syncing is NOT enabled, after adding the directory you will need to select users from the folders within the directory and manually import them.

Important

You will NOT be able to change the **Directory Sync** setting after adding the directory.

4. Click **SELECT**.

   The **Create New Directory** page opens. For example:



5. Configure the following Directory Settings:

- **Name:** Name by which the directory is known.
- **Password:** The password for the administrative user account.
- **Base DN:** The distinguished name of the directory from which users will be added to the system. If you want to add only a specified set of users, enter the relevant node(s) of the directory.
- **User DN:** The username and distinguished name of the administrative user account that allows access to import from the directory.
- **Domain:** The IP address or NetBIOS domain name of the domain.

> **Note**
>
> **For AD only:** A domain value must be entered in order to enable users to authenticate to Windows using a FIDO key.

- **Email Mapping:** The field in the corporate directory used to retrieve the emails of users. Select the mapping source from the list. Keep in mind that you will NOT be able to update the mapping source after directory settings are saved.
- **Host Name/URL:** Select LDAP or LDAPS. Then, in the **Host** field, enter the FQDN of the domain. In the **Port** field, enter **389** for LDAP or **636** for LDAPS.
- **Certificate:** If you are using LDAPS, click **Upload Certificate** and select the relevant certificate file.

6. If you are adding a **ForgeRock Cloud** directory, enter these settings in the appropriate fields:
   - **Service Account Id:** Copy this value from the **Service Accounts** page of the ForgeRock Identity Cloud Admin UI (under **Tenant Settings**).
   - **Service Account Private Key:** Copy this value from the **Service Accounts** page of the ForgeRock Identity Cloud Admin UI (under **Tenant Settings)**.
   - **Service Account Access Token URL:** Enter the Oauth2 access token URL in the following format:

     https://<tenant-env-fqdn>:443/am/oauth2/access_token

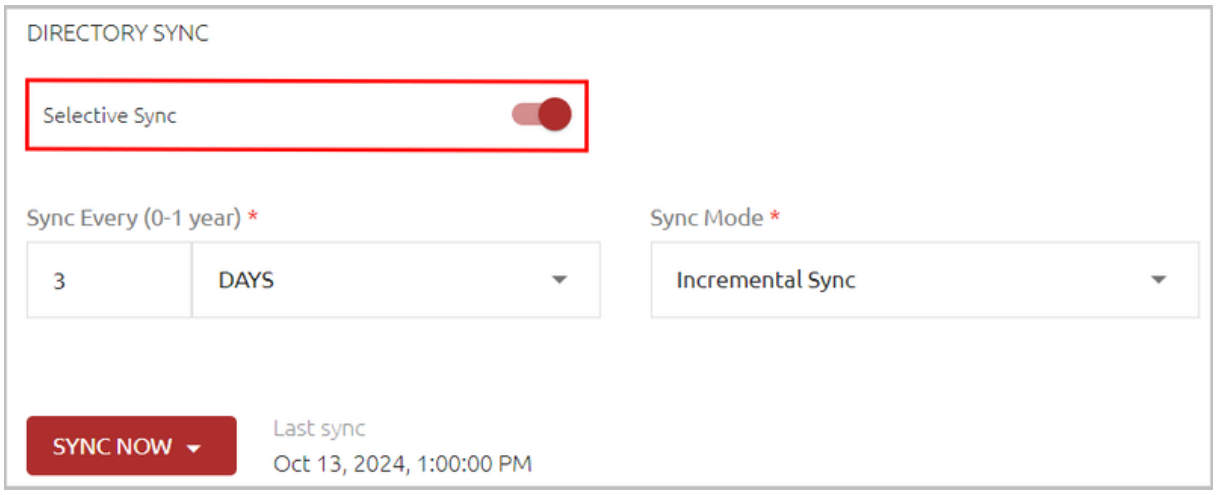
     For further information please refer to this article.
   - **ForgeRock AM URL:** The public AM URL.
   - **ForgeRock IDM URL:** The public IDM URL.
   - **Realm:** The IDM realm being used.
   - **Group Object Name:** Use the value set in your ForgeRock environment. (The default setting is **Role**.)
7. Click **Test Connection** to perform a validity check.

8. At the bottom of the page, click **Create**. Then, from the toolbar at the top of the page, click **PUBLISH** and publish your changes.

9. **For AD directory types with Automatic Sync**, it is recommended to enable Selective Sync in the directory settings:

   a. From the **Directories** menu, click ✎ in the row or tile of the relevant directory to open the directory settings.

   b. Scroll to the bottom of the **Details** tab. Under **Directory Sync**, enable the **Selective Sync** toggle button.



   c. Click **Save**.

Next Steps

Installation and basic configuration of the Enterprise Connect Passwordless authentication system is now completed. The following stages involve adding new services and inviting users to enroll.

To continue to configure your system, refer to the Enterprise Connect Passwordless Management Console Admin Guide.

Appendix A: Authentication Server Sanity Check

After installation of the All-in-One system has completed, you may want to perform the Authentication Server Sanity Check before continuing to configure the system. The Sanity Check is not mandatory. Do it only if you suspect that something went wrong during setup, or if you want to be sure you performed all the required tests.

The Sanity Check includes the following tests:

- Authentication Server installed version:

  ```
  sudo cat /opt/sdo/.sdover
  ```

```
[root@lmesn-mc1 chent]# cat /opt/sdo/.sdover
6.8-b0085
[root@lmesn-mc1 chent]#
```

- Authentication Server engines:

  `sudo systemctl status sdo sdomon sdomcbe`

```
[chent      ]-19 ~]$ sudo systemctl status sdo sdomon sdomcbe
● sdo.service - SDO authentication server
   Loaded: loaded (/etc/systemd/system/sdo.service; enabled; vendor preset: disabled)
   Active: active (running) since Wed 2023-07-05 16:18:07 IDT; 4 days ago
 Main PID: 8825 (node)
   CGroup: /system.slice/sdo.service
           └─8825 /usr/bin/node enroller.js

Jul 10 15:03:07          sdoenroller[8825]: no messages
Jul 10 15:03:12          sdoenroller[8825]: no messages
Jul 10 15:03:17          sdoenroller[8825]: no messages
Jul 10 15:03:22          sdoenroller[8825]: no messages
Jul 10 15:03:27          sdoenroller[8825]: no messages
Jul 10 15:03:33          sdoenroller[8825]: no messages
Jul 10 15:03:38          sdoenroller[8825]: no messages
Jul 10 15:03:43          sdoenroller[8825]: no messages
Jul 10 15:03:48          sdoenroller[8825]: no messages
Jul 10 15:03:53          sdoenroller[8825]: no messages

● sdomon.service - SDO service monitor
   Loaded: loaded (/etc/systemd/system/sdomon.service; enabled; vendor preset: disabled)
   Active: active (running) since Wed 2023-07-05 19:35:32 IDT; 4 days ago
 Main PID: 25162 (node)
   CGroup: /system.slice/sdomon.service
           ├─25162 /usr/bin/node redis_mon.js
           ├─25176 node ./saml.js eyJwb3J0IjozMzM0LCJ0eXBlIjoic2FtbCJ9
           ├─25177 node ./rest.js eyJ0eXBlIjoicmVzdCJ9
           ├─25178 node ./adpa.js eyJ0eXBlIjoiYWRwYSJ9
           ├─25184 node ./rpc.js eyJ0eXBlIjoicnBjIn0=
           ├─25226 /usr/bin/node /opt/sdo/authserver/saml.js eyJwb3J0IjozMzM0LCJ0eXBlIjoic2FtbCJ9
           ├─25227 /usr/bin/node /opt/sdo/authserver/saml.js eyJwb3J0IjozMzM0LCJ0eXBlIjoic2FtbCJ9
           ├─25244 /usr/bin/node /opt/sdo/authserver/rpc.js eyJ0eXBlIjoicnBjIn0=
           ├─25245 /usr/bin/node /opt/sdo/authserver/adpa.js eyJ0eXBlIjoiYWRwYSJ9
           ├─25246 /usr/bin/node /opt/sdo/authserver/rpc.js eyJ0eXBlIjoicnBjIn0=
           ├─25247 /usr/bin/node /opt/sdo/authserver/adpa.js eyJ0eXBlIjoiYWRwYSJ9
           ├─25250 /usr/bin/node /opt/sdo/authserver/rest.js eyJ0eXBlIjoicmVzdCJ9
           └─25263 /usr/bin/node /opt/sdo/authserver/rest.js eyJ0eXBlIjoicmVzdCJ9
```

- Authentication Server log engines:

  `sudo systemctl status elasticsearch logstash`

```
[chent@      19 ~]$ sudo systemctl status elasticsearch logstash
● elasticsearch.service - Elasticsearch
   Loaded: loaded (/usr/lib/systemd/system/elasticsearch.service; enabled; vendor preset: disabled)
  Drop-In: /etc/systemd/system/elasticsearch.service.d
           └─override.conf
   Active: active (running) since Wed 2023-07-05 16:18:05 IDT; 4 days ago
     Docs: https://www.elastic.co
 Main PID: 8449 (java)
   CGroup: /system.slice/elasticsearch.service
           ├─8449 /usr/share/elasticsearch/jdk/bin/java -Xshare:auto -Des.networkaddress.cache.ttl=60 -Des.networ
           └─8671 /usr/share/elasticsearch/modules/x-pack-ml/platform/linux-x86_64/bin/controller

Jul 05 16:17:34          systemd[1]: Stopped Elasticsearch.
Jul 05 16:17:34          systemd[1]: Starting Elasticsearch...
Jul 05 16:18:05          systemd[1]: Started Elasticsearch.

● logstash.service - logstash
   Loaded: loaded (/etc/systemd/system/logstash.service; enabled; vendor preset: disabled)
   Active: active (running) since Wed 2023-07-05 16:18:06 IDT; 4 days ago
 Main PID: 8793 (java)
   CGroup: /system.slice/logstash.service
           └─8793 /usr/share/logstash/jdk/bin/java -Xms1g -Xmx1g -XX:+UseConcMarkSweepGC -XX:CMSInitiatingOccupan

Jul 05 16:19:16          logstash[8793]: [2023-07-05T16:19:16,930][INFO ][logstash.outputs.elasticsearch][main] E
Jul 05 16:19:16          logstash[8793]: [2023-07-05T16:19:16,935][WARN ][logstash.outputs.elasticsearch][main] D
Jul 05 16:19:17          logstash[8793]: [2023-07-05T16:19:17,200][INFO ][logstash.outputs.elasticsearch][main] C
Jul 05 16:19:17          logstash[8793]: [2023-07-05T16:19:17,270][INFO ][logstash.outputs.elasticsearch][main] U
Jul 05 16:19:17          logstash[8793]: [2023-07-05T16:19:17,274][INFO ][logstash.outputs.elasticsearch][main] C
Jul 05 16:19:17          logstash[8793]: [2023-07-05T16:19:17,522][INFO ][logstash.javapipeline    ][main] Starti
Jul 05 16:19:18          logstash[8793]: [2023-07-05T16:19:18,981][INFO ][logstash.javapipeline    ][main] Pipeli
Jul 05 16:19:19          logstash[8793]: [2023-07-05T16:19:19,331][INFO ][logstash.inputs.tcp       ][main][ba443f
Jul 05 16:19:19          logstash[8793]: [2023-07-05T16:19:19,349][INFO ][logstash.javapipeline    ][main] Pipeli
Jul 05 16:19:19          logstash[8793]: [2023-07-05T16:19:19,554][INFO ][logstash.agent           ] Pipelines ru
Hint: Some lines were ellipsized, use -l to show in full.
```

- Authentication Server database:

  `sudo systemctl status redis`

```
[chent        ~]$ sudo systemctl status redis
● redis.service - Redis persistent key-value database
   Loaded: loaded (/usr/lib/systemd/system/redis.service; enabled; vendor preset: disabled)
  Drop-In: /etc/systemd/system/redis.service.d
           └─limit.conf
   Active: active (running) since Wed 2023-07-05 16:12:44 IDT; 4 days ago
 Main PID: 7950 (redis-server)
   CGroup: /system.slice/redis.service
           └─7950 /usr/bin/redis-server 127.0.0.1:6379

Jul 05 16:12:44          systemd[1]: Starting Redis persistent key-value database...
Jul 05 16:12:44          systemd[1]: Started Redis persistent key-value database.
```

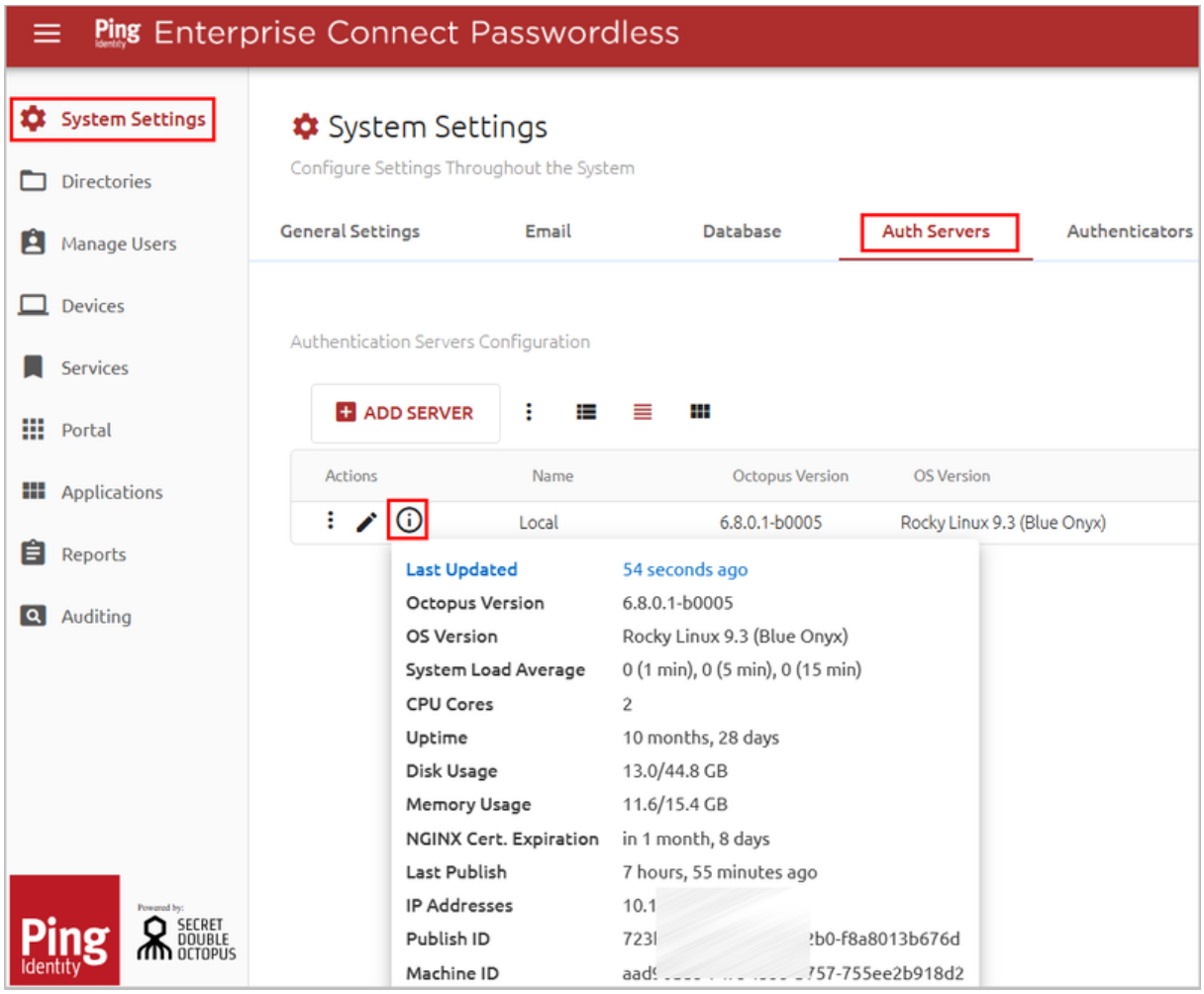
- Authentication Server Web engine:

  `sudo systemctl status nginx`

```
[chent        9 ~]$ sudo systemctl status nginx
● nginx.service - nginx - high performance web server
   Loaded: loaded (/usr/lib/systemd/system/nginx.service; enabled; vendor preset: disabled)
  Drop-In: /etc/systemd/system/nginx.service.d
           └─override.conf
   Active: active (running) since Wed 2023-07-05 16:17:11 IDT; 4 days ago
     Docs: http://nginx.org/en/docs/
 Main PID: 8094 (nginx)
   CGroup: /system.slice/nginx.service
           ├─8094 nginx: master process /usr/sbin/nginx -c /etc/nginx/nginx.conf
           ├─8095 nginx: worker process
           └─8096 nginx: worker process

Jul 05 16:17:11          systemd[1]: Starting nginx - high performance web server...
Jul 05 16:17:11          systemd[1]: Started nginx - high performance web server.
```

Appendix B: Server Health Checks

If you suspect that the Authentication Server is not functioning properly, you may want to perform the server health checks listed below. Keep in mind that you can also view detailed data about a selected Authentication Server in the Management Console (**System Settings > Auth Servers**).



- OS version and packages:

  ```
  sudo uname -a
  sudo hostnamectl
  ```

- OS packages installation:

  ```
  yum install net-tools
  ```

  The following checks are applicable for CentOS:

  ```
  yum install epel-release
  sudo rpm --query centos-release
  ```

- Running processes:

```
ps -ef | grep sdo
sudo top
sudo systemctl status
```

- Network configuration:

```
sudo ip addr
```

- Machine memory and partitions:

```
sudo df -k
sudo free -h
```

- Machine's log trace:

```
sudo journalctl -b
```

- Firewall daemon status and port-table:

```
sudo systemctl status firewalld
sudo firewall-cmd --list-all
```

- Security Enhancement (SELINUX) configuration:

```
cat /etc/selinux/config
```

Appendix C: Database Configuration

By default, installation of the Management Console creates a local PostgreSQL DB. If the installer chooses not to create the default database, the database connection needs to be configured manually following installation.

If a database was not added during installation, the **Database** tab opens when you log into the Management Console for the first time. In addition, the following warning message is displayed: "No database is configured. Configure a database in order to proceed."

Database User Permission Requirements

Required user permissions for each supported database type are listed in the table below.

Important

If you are working with multiple Management Console Servers, **the same database user** must be used for all instances.

Database Type	User Permissions
MS SQL (SQL Server Authentication)	• **Server Roles:** public (sysadmin optional) • **Database Role:** public, db_owner
Oracle	• Grant connect to <user> • Grant all privileges to <user>

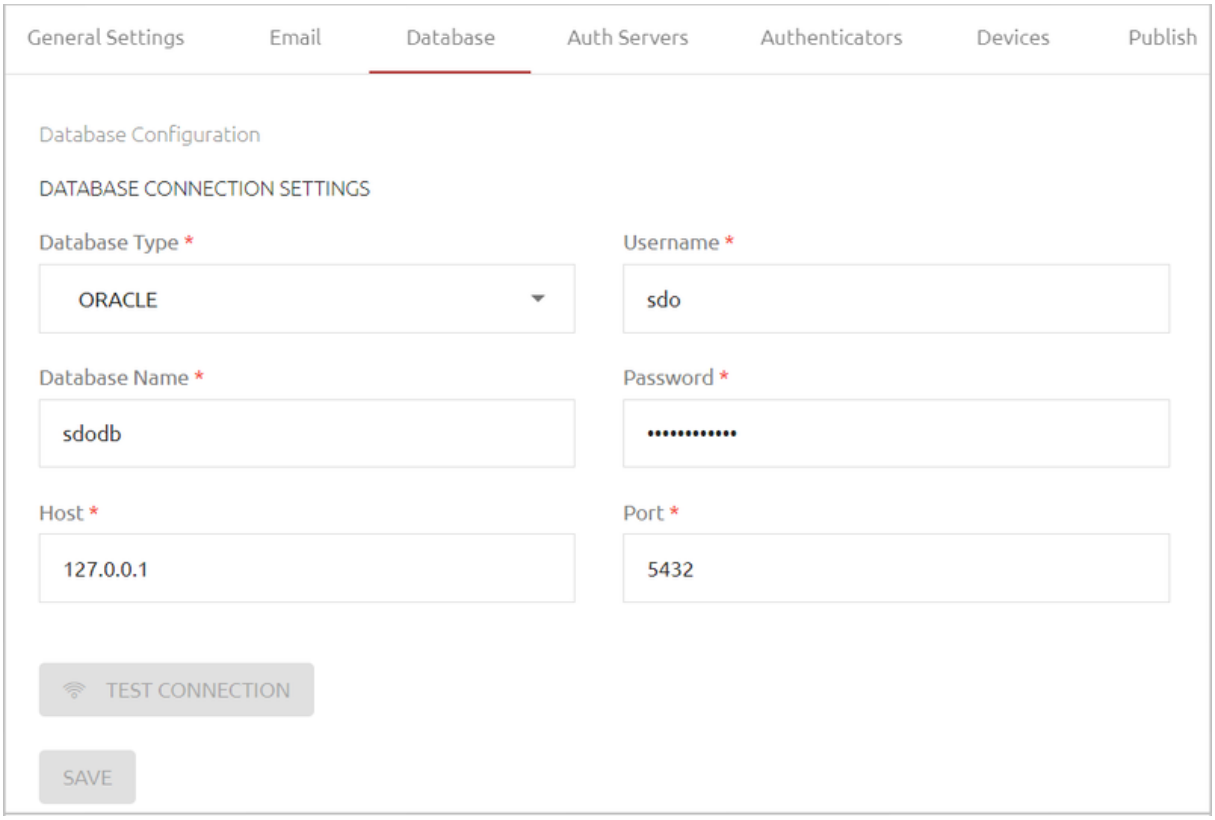
Database Type	User Permissions
PostgreSQL	Grant all privileges on database <db> to <user>

Configuring the Database Connection

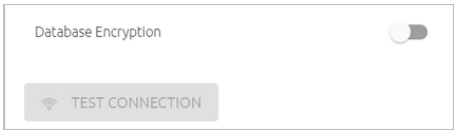
The database connection is easily configured from the Management Console.

To configure the database connection:

1. From the **System Settings** menu of the Management Console, select the **Database** tab.



2. From the **Database Type** list, select **PostgreSQL**, **MS SQL** or **Oracle**.
3. Specify the following settings by entering the relevant values in the appropriate fields:
    - **Database Name:** Name of the database
    - **Host and Port:** IP address (or URL) and port of the database
    - **Username and Password:** Credentials of the database administrator
4. **For MS SQL database types only:** If the connection to the database is encrypted, enable the **Database Encryption** toggle button.



5. **For PostgreSQL database types only:** To enable SSL communication between the Authentication Server and an external database, enable the **SSL Connection** toggle button.

6. To check validity of your settings, click **Test Connection**.
7. To save the settings, click **Save** and then publish your changes.

Appendix D: Replacing the SSL Certificate for Nginx

To establish Nginx communications on a secure tunnel, Secret Double Octopus recommends enforcing a root-CA certificate, thus assuring an SSL connection with the Authentication Server.

The Authentication Server supports the following Nginx engines:

- Web Nginx for SAML web services
- Authentication Management Nginx

Prerequisites

Before you begin, verify that the Authentication Server's hostname is running FQDN:

```
# hostnamectl set-hostname OctopusAuthenticationFQDN.com --static
```

SSL Certificate for Nginx

The SSL certificate allows access to the Nginx web engine through an encrypted secured connection. TLS/SSL works by using a combination of a public certificate and a private key:

- The **SSL key** is kept a secret on the server. It is used to encrypt content sent to clients.
- The **SSL certificate** is publicly shared with anyone requesting the content. It can be used to decrypt the content signed by the associated SSL key.

Approved SSL vendors can issue validated SSL certificates.

The following sections describe how to create and configure the SSL certificate. If you have already done this, skip to the instructions for replacing the certificate.

Creating the OpenSSL File and Generating the CSR

By default, the OpenSSL does not include an alternate subject name (which is required for verification on Chrome browse v58 and up). To create a certificate that includes the alternate subject name, a config file has to be created and used when requesting the certificate.

Create a config file named (for example) **san.cnf** with the following information:

```
[ req ]
default_bits = 2048
distinguished_name = req_distinguished_name
req_extensions = req_ext
[ req_distinguished_name ]
countryName = Country Name (2 letter code)
stateOrProvinceName = State or Province Name (full name)
localityName = Locality Name (eg, city)
organizationName = Organization Name (eg, company)
commonName = Common Name (e.g. server FQDN or YOUR name)
[ req_ext ]
subjectAltName = @alt_names
[alt_names]
DNS.1 = <server FQDN>
```

After creating the file, generate a certificate signing request (CSR):

```
# sudo openssl req -new -newkey rsa:2048 -nodes -config san.cnf
-keyout selfsigned.key -out selfsigned.csr
```

You will be asked to enter the certificate information that will be incorporated into your certificate request. Please **use only alphanumeric characters** when completing the details.

To verify that the CSR file contains the alternate subject name, run the following:

```
openssl req -noout -text -in selfsigned.csr | grep DNS
```

SSL Certificate Activation

Next, use the CSR file to submit a request for corporate SSL certificate activation (CA Authority validation):

1. **Submit the SSL Certification Request:** Open the Certificate Signing Request (CSR) file with the text editor, copy its content together with the header "-----BEGIN CERTIFICATE REQUEST-----" and footer "-----END CERTIFICATE REQUEST-----" and use it to activate the certificate in your corporate's Certificate Authority account.

2. **Sign with MS CA:** On your domain machine, open the command line as an admin and run the following:

   ```
   certreq -submit -attrib "CertificateTemplate:webServer"
   selfsigned.csr selfsigned.cer
   ```

Installing and Configuring Your SSL Certificate

Following certificate activation, you will receive your issued Domain-Name Certificate pem file (**server.crt**). This file contains the Primary Root CA certificate (**ca.crt**) file and the Intermediate certificate.

For a valid Nginx SSL Certificate, you need to concatenate your Bundle certificate together with your Obtain certificate into a single unified .crt file (e.g., **selfsigned.crt**):

```
# cat server.crt ca.crt > selfsigned.crt
```

Then perform the following steps:

1. As a root user, copy the certificate and the key to the **nginx** folder:

   ```
   # cp selfsigned.crt /etc/pki/nginx/
   # cp selfsigned.key /etc/pki/nginx/private/
   ```

2. Restart the server:

   ```
   # sudo systemctl restart nginx
   ```

3. Perform a sanity check:

   ```
   # sudo nginx –t
   ```

Verifying Nginx Encryption

To check for successful encryption, open your web browser and enter the following in the address bar:

https://<Authentication Server domain name>

Verify that the page loads with no security warning.

Replacing the SSL Certificate

Steps for Management Console Servers:

1. Navigate to **cd /etc/nginx/conf.d/** and run the following command:

   ```
   cat sdomcbe.conf
   ```

2. Check the server path. Be sure to create a copy of all the files before editing them.

   ```
   ssl_certificate /etc/pki/nginx/
   server_certificate_for_example.crt;
   ssl_certificate_key /etc/pki/nginx/private/
   server_certificate_key_for_example .key;
   ```

3. Change the owner of the new files to *sdo*:

   ```
   cd /etc/pki/nginx/
   chown sdo:sdo server_certificate_for_example.crt
   cd /etc/pki/nginx/private/
   chown sdo:sdo server_certificate_key_for_example .key
   ```

4. Restart the server:

```
systemctl restart nginx sdomcbe
```

Steps for Authentication Servers and DMZ Servers:

1. Navigate to **cd /etc/nginx/conf.d/sdomon.conf** and run the following command:

   ```
   cat sdomon.conf
   ```

2. Check the server path. Be sure to create a copy of all the files before editing them.

   ```
   ssl_certificate /etc/pki/nginx/
   server_certificate_for_example.crt;
   ssl_certificate_key /etc/pki/nginx/private/
   server_certificate_key_for_example .key;
   ```

3. Change the owner of the new files to *sdo*:

   ```
   cd /etc/pki/nginx/
   chown sdo:sdo server_certificate_for_example.crt
   cd /etc/pki/nginx/private/
   chown sdo:sdo server_certificate_key_for_example .key
   ```

4. Restart the server:

   ```
   systemctl restart nginx sdomon sdotun
   ```

Appendix E: Logstash and Elasticsearch Folder with No Execution Permission

Logstash and Elasticsearch use the **/tmp** folder to temporarily store some modules and execute them. This causes issues with installations that have the **/tmp** folder mounted with *noexec*. If this situation is detected, the installation will notify the user about the recommended course of action.

During the installation process, the Admin should allow the **/tmp** folder to execute by using the *TMPDIR* environment variable to override the default temporary folder. This will allow the installation to complete with no errors.

After the installation is complete, the Admin should change the global parameter to a different folder that will be used as the temp for these modules. To do so, follow these steps:

1. Add *-Djava.io.tmpdir=<tmp dir>* to
   - **/etc/logstash/jvm.options**
   - **/etc/elasticsearch/jvm.options**
2. Restart the services by running the following command:

   ```
   sudo systemctl restart logstash elasticsearch
   ```

Appendix F: Moving Elasticsearch Data and Logs to a New Directory

This section explains how to move installed Elasticsearch directories, using default locations.

Before you begin, make sure that you have:

- SUDO access
- A backup of the **/etc/elasticsearch/elasticsearch.yml** file

Follow the steps below to move Elasticsearch data. Migrating logs is optional and relevant instructions appear in parentheses.

To move Elasticsearch data (and logs):

1. Determine the current location of your data files by running the following command:

   ```
   > curl "localhost:9200/_nodes/settings?pretty=true"
   ```

   The default folders are **/var/lib/elasticsearch** and **/var/logs/elasticsearch**

2. Create a new directory structure. For example:

   ```
   > cd /opt/<new location>/ > mkdir elsdata
   ```

   (If you want to migrate the logs, create an additional folder *mkdir elslogs*)

3. Stop the sdomcbe service by running the following command:

   ```
   > systemctl stop sdomcbe
   ```

4. Stop the Elasticsearch service by running the following command:

   ```
   > systemctl stop elasticsearch
   ```

5. Navigate to the current data directory (as determined in Step 1), and copy files to the new location. For example:

   ```
   cp –RP * /opt/<new location>/elsdata/
   ```

   (If you are migrating the logs, copy those files to *elslogs*)

6. Change ownership on the new directory to Elasticsearch:

   ```
   > chown –R elasticsearch:elasticsearch /opt/<new location>/
   elsdata/
   ```

   (If you are migrating logs, run the same command for *elslogs*)

7. Change ownership on the **sdo** directory to *sudo chmod o+rx /opt/sdo/*

8. Edit the data path of the **elasticsearch.yml** file:

   ```
   > vi /etc/elasticsearch/elasticsearch.yml
   ```

   Change the *path.data* data parameter to *path.data:/opt/<new location>/elsdata/*

(If you are migrating logs, change the *path.logs* data parameter as well.)

9. Start the Elasticsearch service by running the following command:

   ```
   > systemctl start elasticsearch.service
   ```

10. Start the sdomcbe service by running the following command:

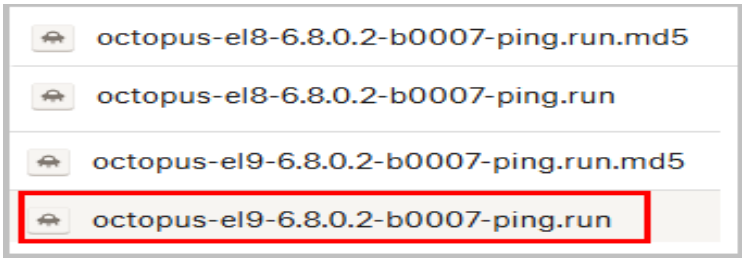
    ```
    > systemctl start sdomcbe
    ```

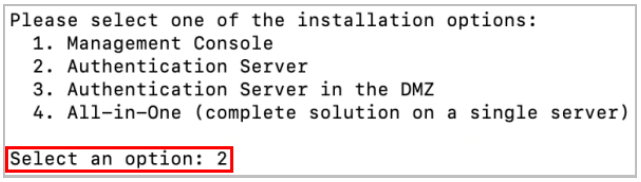
Appendix G: Upgrading Your System to Red Hat 9.x

In the event that you need to upgrade your entire solution from Red Hat version 8.x to 9.x, follow the instructions below. This method of upgrade allows you to rebuild your entire distributed server configuration without interruptions in system operation.

To upgrade a distributed configuration to Red Hat 9.x:

1. Install a *new* machine with Red Hat version 9.x.
2. Install an Authentication Server on the new machine using the installation package for version 6.8. Be sure to run the **el9** flavor installation script and select installation option **2**.





   Connect the new Authentication Server to your existing primary Management Console Server. For details, refer to Authentication Server Installation.

3. Install another *new* machine with Red Hat version 9.x.
4. Install a DMZ Server on the new machine using the installation package for version 6.8. Be sure to run the **el9** flavor installation script and select installation option **3**.

   Connect this DMZ Server with the new Authentication Server that you created in Step 2. For details, refer to DMZ Installation.

5. Test the new installation and verify that the server is operating as expected.

6. Disconnect an Authentication Server on a machine running version 8.x from the Load Balancer, and delete the machine.

7. Install a *new* machine with Red Hat version 9.x. Then install a new Authentication Server on the machine using the installation package for version 6.8, as described in Step 2.

8. Delete the machine running the DMZ Server that was associated with the old Authentication Server.

9. Install a *new* machine with Red Hat version 9.x. Then install a new DMZ Server on the machine using the installation package for version 6.8, and connect it with the Authentication Server that you created in Step 7.

10. Connect the new Authentication Server to the Load Balancer.

11. Repeat Steps 5-9 for each old Authentication Server in your environment.

12. Install a *new* machine with Red Hat version 9.x.

13. Install a *new* secondary Management Console Server on the machine using the installation package for version 6.8. Be sure to run the **el9** flavor installation script, select installation option **1**, and specify secondary MC installation.

    Connect the new secondary Management Console Server to your existing primary Management Console Server. For details, refer to Secondary MC Server Installation.

14. Run the script to change the secondary Management Console Server to the main one. Then, kill the old primary server and delete the machine.

15. Install a *new* machine with Red Hat version 9.x.

16. Install a secondary Management Console Server on the machine using the installation package for version 6.8. Connect it to the new primary Management Console Server that you configured in Step 13.

Appendix H: Guidelines for Installing OS Updates and Patches

The Red Hat and Oracle Linux operating systems generally utilize many different permutations of RPMs. Occasionally when vulnerabilities are identified, it is necessary to update or patch some of the OS RPMs.

In order to avoid system downtimes, interruptions in workflows and other issues associated with the new RPMs, **we strongly recommend following these best practice guidelines**:

1. Before working with patches or new RPMs, always perform a backup or take a snapshot of the server.

2. Before installing in the production environment, always test new RPMs in a development or testing environment that is identical to the production environment.

If you encounter any unexpected issues, please contact Customer Support for assistance.