ADSelfService Plus

Post-deployment security measures

ManageEngine
ADSelfService Plus

www.adselfserviceplus.com

Table of Contents

1 Introduction

After the deployment of ADSelfService Plus, there are a few measures that have to be carried out for a secure inbound connection between the ADSelfService Plus server, the user's web browser, or the ADSelfService app. It is also important to protect the outbound connection between the ADSelfService Plus server, the mail server, and the external database server. The ADSelfService Plus installation directory must also be guarded against access by unauthorized users.

This guide details the various steps for implementing these measures and protecting the ADSelfService Plus deployment in your enterprise.

2 Security features that need to be enabled during inbound connections

After the deployment of ADSelfService Plus, there are a few measures that have to be carried out for a secure inbound connection between the ADSelfService Plus server, the user's web browser, or the ADSelfService app. It is also important to protect the outbound connection between the ADSelfService Plus server, the mail server, and the external database server. The ADSelfService Plus installation directory must also be guarded against access by unauthorized users.

This guide details the various steps for implementing these measures and protecting the ADSelfService Plus deployment in your enterprise.

1. Configure SSL, and add ciphers and protocols

i. SSL configuration

To protect the data transferred between the ADSelfService Plus server, the user's web browser, and the ADSelfService Plus app, and to secure data during application programming interface (API) access, Secure Sockets Layer (SSL) certificates should be installed, and an HTTPS connection should be configured.

Check out the complete guide on how to configure SSL for ADSelfService Plus.

ii. Add ciphers and protocols

Specific ciphers and protocols can be used to enable forward secrecy. Forward secrecy protects previously recorded traffic between the user's web browser and the ADSelfService Plus server from being decrypted and misused. To configure forward secrecy, add the necessary ciphers and protocols to the server.xml file using these steps:

1. Open the server.xml file, located in the <Install_directory>/conf folder.
   Locate the following connector tag:

```
<Connector SSLEnabled="true"
```

2. Add the following ciphers and protocols to the connector tag:

```
protocol="org.apache.coyote.http11.Http11NioProtocol"
ciphers="TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384,
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384"
allowUnsafeLegacyRenegotiation="false"
server="Adselfservice Plus"
sslProtocol="TLS"
compression="off"
```

```
SSLEnabledProtocols="TLSv1.2"
```

For example:

```
<Connector SSLEnabled="true" acceptCount="100" compression="off"
protocol="org.apache.coyote.http11.Http11NioProtocol"
ciphers="TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384,
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384"
clientAuth="false" connectionTimeout="-1" debug="0"
disableUploadTimeout="true" enableLookups="false"
keystoreFile="./conf/server.keystore" keystorePass="adventnet"
maxSpareThreads="75" maxThreads="150" minSpareThreads="25"
name="SSL" port="9251" scheme="https" secure="true"
allowUnsafeLegacyRenegotiation="false" server="AdselfservicePlus"
sslProtocol="TLS" sslEnabledProtocols="TLSv1.2"/>
```

2. Apply security parameters

Security parameters define the headers of the HTTP response messages from the ADSelfService Plus server. They help mitigate attacks by instructing the end user's web browser how to handle the content provided by the server. Security parameters protect communication between the server and the web browser by:

1. Preventing the web browser from caching the server response.
2. Preventing XSS (cross-site scripting) attacks.
3. Allowing only HTTPS connections and restricting HTTP connections.
4. Preventing clickjacking.

Follow these steps to successfully apply the security parameters:

1. Download the security parameters file from here.
2. Go to the ***<Install_directory>/conf*** folder, and place the downloaded file in it.

Note: Modify the Content Security Policy header

The Content-Security-Policy header is used to define trusted sources for the resources to be rendered on a web page. Once these sources are defined, only resources from them can be executed on the web page. By default, under the Content-Security-Policy header in the ***security_params.conf*** file, the ADSelfService Plus server and the Duo Security application are the only sources that are defined as trusted resources for content rendered in the ADSelfService Plus portal.

Policy directives help decide what content the source is allowed to execute. A few policy directives that are used in the security_params.conf file are:

frame-src - Defines the trusted sources for HTML frame resources. img-src - Defines the trusted sources for image resources. script src - Defines the trusted sources for Javascript resources. style-src - Defines the trusted sources for stylesheets. default-src - Defines the trusted sources for all kinds of resources.

In the existing ***security_params.conf*** file 'self' is defined as the trusted source for the rendered resources. The source 'self' refers to the origin of the web page. In our case, it refers to the server where ADDSelfService Plus is deployed. Here is the existing Content-Security-Policy header:

```
Content-Security-Policy=default-src 'self' ; script-src 'self' 'unsafe-inline'
'unsafe-eval' ; connect-src 'self' ; img-src 'self' ; style-src 'self'
'unsafe-inline'; frame-src 'self' https://*.duosecurity.com/ ;
```

For improved security, organizations can replace the source from 'self' to the exact domain address of the origin domain. In case any other domain gets designated as the origin, this prevents the content of that domain from being executed in the ADSelfService Plus portal. Consider an example where ADSelfService Plus is deployed in the domain abcdcorp.com in an organization. This domain can be exclusively defined as the source for the content executed by replacing 'self' with the domain's complete domain address as mentioned below:

```
Content-Security-Policy=default-src https://*.abcdcorp.com ; script-src
https://*.abcdcorp.com  'unsafe-inline' 'unsafe-eval' ; connect-src
https://*.abcdcorp.com  ; img-src https://*.abcdcorp.com ; style-src
https://*.abcdcorp.com  'unsafe-inline'; frame-src https://*.abcdcorp.com
https://*.duosecurity.com/ ;
```

3. Set cookies to HttpOnly

Setting cookies to HttpOnly permits only the ADSelfService Plus server to access the cookies and blocks any script from the web browser side from accessing it. To set the cookies to HttpOnly run the following query in the database:

```
"insert into systemparams values((select max(system_param_id) from
systemparams)+1,'ENABLE_HTTPONLY','true');"
```

Note:

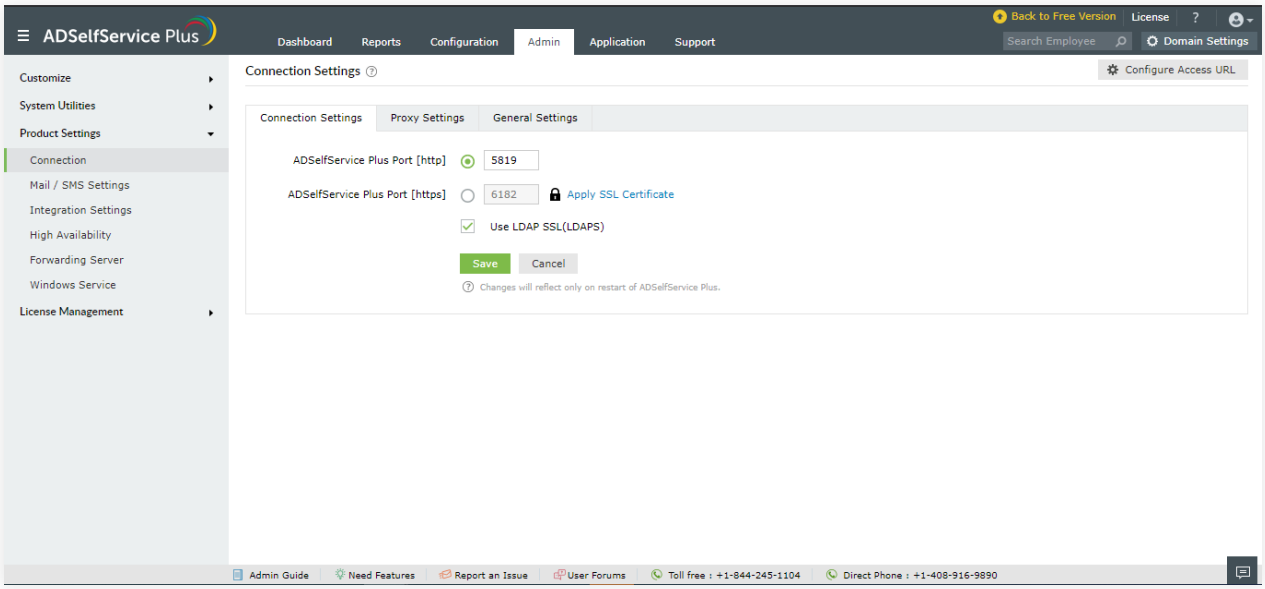
Since the adscsrf and _zcsr_tmp cookies are required to be accessed by the web browser for the functioning of the ADSelfService Plus portal, HttpOnly will not be set for them.

3 Measures to promote security during outbound connections:

1. Enable LDAPS

When the Active Directory domain controller has SSL enabled (recommended), a Secure Lightweight Directory Application Protocol (LDAPS) connection can be configured in the ADSelfService Plus Connection settings to ensure a secure connection between ADSelfService Plus and Active Directory. Follow these steps to enable LDAPS connection:

1. In the *ADSelfService Plus administrator portal*, open the **Admin** tab.
2. Go to **Connection (Admin > Product Settings > Connection).**
3. Check the **Use LDAP SSL (LDAPS)** box.
4. Click **Save.**



2. Configure an SSL/TLS connection with the mail server

After deploying the mail server with a specific protocol (SSL/TLS), you need to configure the same protocol in the ADSelfService Plus Mail Server settings. This is done to establish a secure connection between the ADSelfService Plus server and the mail server. Check out this article for details on how to enable an SSL/TLS connection between ADSelfService Plus and the mail server.

3. Configure an SSL connection with MS SQL Server

ADSelfService Plus supports MS SQL in addition to the built-in PostgreSQL. To secure the data transferred between the ADSelfService Plus server and MS SQL Server, it is necessary to configure an SSL connection between them. This is done by applying an SSL certificate in SQL Server. This guide offers a detailed explanation on how to secure the connection between ADSelfService Plus and MS SQL using SSL.

4 Configure file permissions for the ADSelfService Plus installation directory

The ADSelfService Plus installation directory contains important files and folders, including the license file and files that are used to start and stop the product. Administrators need to be provided with file permissions to the folder where the installation directory is located (for example, the ***C:\ManageEngine*** folder) to be able to access and modify the folder contents.

Assigning **Full Control** permissions gives the administrator all the access they need and more. However, this may lead to security vulnerabilities. To overcome this, we recommend delegating only the permissions they need by following the steps in this document.