Active Directory (ADFS)

SupportPro Configuration

1. Download the below file, extract the saml.php file from the zip archive and place it inside the config/production of your SupportPro installation directory.

2. On your SupportPro server create a signing certificate that you will need for the ADFS logout request.

```
openssl req -x509 -nodes -sha256 -days 730 -new
key rsa:2048 -keyout /etc/pki/tls/private/mysig
ning.key -out /etc/pki/tls/certs/mysigning.pem
```

    1. Update config/production/saml.php with the certificate and key information.
        1. Replace X_PASTE_SUPPORTPro_SIGNING_CERT_HERE with the contents of /etc/pki/tls/certs/mysigning.pem
        2. Replace X_PASTE_SUPPORTPro_SIGNING_CERT_PKEY_HERE with the contents of /etc/pki/tls/private/mysigning.key
    2. Replace $ADFSSERVER in the saml.php file with your ADFS server information

ADFS Server Configuration

Authentication Guards

SupportPro allows separate authentication guards to be configured for frontend and operator login, see: . Please repeat this step if you would like to configure both frontend and operator login.

1. On your ADFS server, open the ADFS Management Console
2. Select ADFS > Relying Party Trust > Add Relying Party Trust
    1. Select Claims aware and click Next
    2. Select Import data about the relying party published online, and enter your SupportPro SAML metadata URL (see: [redacted])
    3. Set an Access Control policy as you see fit
    4. Name your relay party trust and click Finish to create the trust
3. Select your new relay party trust and select Edit Claim Issuance Policy
    1. Select Add Rule
        1. Select the Send LDAP Attributes as Claims template
        2. Enter a claim rule name
        3. Select Active Directory as your attribute store
        4. Select your attributes
            1. LDAP: E-Mail-Addresses
                1. Outgoing:email
            2. LDAP: Display-Name
                1. Outgoing:fullname
        5. Click Finish
    2. Select Add Rule to add another rule
        1. Select the Transform an Incoming Claim template
        2. Enter a claim rule name
        3. Incoming claim type: Windows Account
        4. Outgoing claim type: Name ID (Persistent Identifier)
        5. Click Finish
4. Select ADFS > Service > Certificates
    1. Double click the Token-signing cert
    2. Select Details > Copy to file

3. Export certificate as base64 without private key
4. Open this file and paste the contents into config/production/saml.php under X_PASTE_ADFS_SIGNING_CERT_HERE