

Netop Remote Control Portal: ADFS and Azure AD Integration

Article Number: 456 | Last Updated: Wed, Aug 22, 2018 10:07 AM

The document attached describes how to configure the Netop Portal for ADFS/Azure AD integration, how to configure the ADFS server/Azure AD and how to use the integration with ADFS/Azure AD. **Benefits of the Netop Portal integration with ADFS/Azure AD: Already existing user data can be used** Instead of manually filling in information for every user, the ADFS/Azure AD integration allows using data from the company's user store. This also means that data from the Netop Portal is synced with the company's data on every user login (name and email). **Authentication based on credentials that the user already knows** The user logging in the Portal will be able to use the same credentials he/she is already using in the various company applications (e.g. email, computer login). This will mean that the password rules will be the same as the ones for the company. **Immediate user termination** In case the user should stop having access to sensitive information (e.g. cease of employment) and gets disabled or removed from the user directory, that user will automatically stop having access to the Netop Portal. **Mixed authentication in the same account** With the introduction of ADFS/Azure AD integration, the Netop Portal account enables multiple authentication types within the same account. That means that some users can continue to have username & password authentication, while others use ADFS/Azure AD. This is highly relevant for scenarios when 3rd party vendors need to get access to devices. At the same time, multi-factor authentication can be added on top of the existing ADFS/Azure AD authentication, thus increasing the overall solution security.

Posted - Wed, May 3, 2017 11:40 AM.

Online URL: <https://kb.netop.com/article/netop-remote-control-portal-adfs-and-azure-ad-integration-456.html>