Managing User Accounts

Virtual Desktop Service

Toby vanRoojen
February 17, 2021

Table of Contents

Managing User Accounts

Create New User(s)

Admins can add Users by clicking Workspaces > Users and Groups > Add/import

Users can be added individually or with a bulk import.

Including accurate email and mobile phone # at this stage greatly improves the process of enabling MFA later.

Once you have created Users, you can click on their name to see details like when they were created, their connection status (whether they're currently logged in or not) and what their specific settings are.

Activating the Virtual Desktop for existing AD users

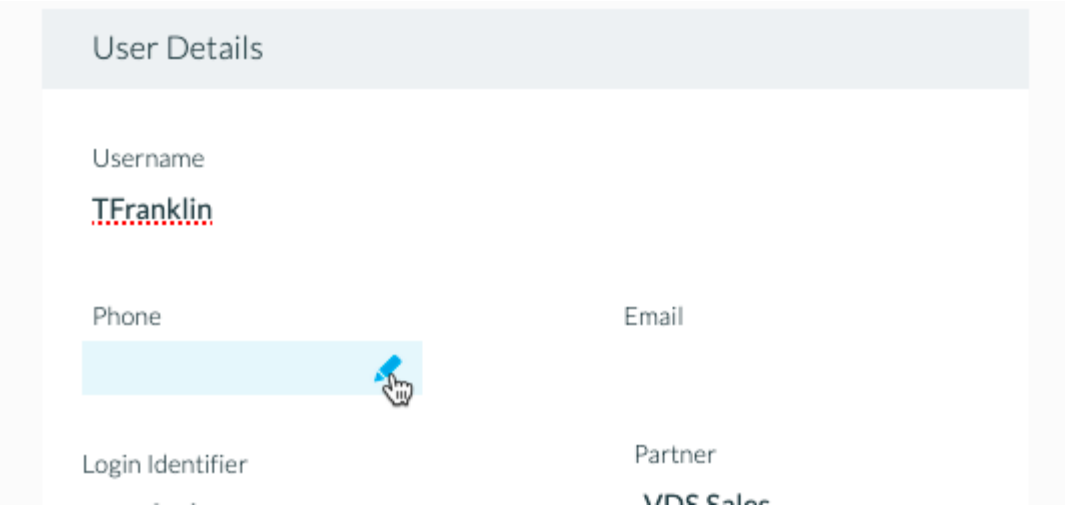
If users are already present in AD, you can simple activate the users' Virtual Desktop by clicking on the gear next to their name and then enabling their desktop.

For Azure AD Domain Service only: In order for logins to work, the password hash for Azure AD users must be synced to support NTLM and Kerberos authentication. The easiest way to accomplish this task is to change the user password in Office.com or the Azure portal, which will force the password hash sync to occur. The sync cycle for Domain Service servers can take up to 20 minutes so changes to passwords in Azure AD typically take 20 minutes to be reflected in AADDS and thus in the VDS environment.

Delete user account(s)

Edit user info

On the user detail page changes can be made the the user details such as username and contact details. The email and phone values are used for the Self Service Password Reset (SSPR) process.



Edit user security settings

- VDI User Enabled – an RDS Setting that, when enabled, builds a dedicated VM session host and assigned this user as the only user that connect to it. As part of activating this checkbox the CWMS administrator is prompted to select the VM Image, Size and Storage Type.
  - AVD VDI users should be managed on the AVD page as a VDI host pool.
- Account Expiration Enabled – allows the CWMS administrator to set an expiration date on the end user account.
- Force Password Reset at Next Login – Prompts the end user to change their password at next login.
- Multi-Factor Auth Enabled – Enables MFA for the end user and prompts them to setup MFA at next login.
- Mobile Drive Enabled – A legacy feature not used in current deployments of RDS or AVD.
- Local Drive Access Enabled – Allows the end user to access their local device storage from the cloud environment including Copy/Paste, USB Mass storage and system drives.
- Wake on Demand Enabled – For RDS users connecting via the CW Client for Windows, enabling this will give the end user permission to take their environment when connecting outside of normal working hours as defined by Workload Schedule.

Locked Account

By default, five failed login attempts will lock the user account. The user account will unlock after 30 minutes unless *Enable Password Complexity* is enabled. With password complexity enabled, the account will not automatically be unlocked. In either case, the VDS admin can manually unlock the user account from the Users/Groups page in VDS.

Reset user password

Resets the user password.

Note: When resetting Azure AD user passwords (or unlocking an account) there can be a delay of up to 20 minutes as the reset propagates through Azure AD.

Admin Access

Enabling this give the end user limited access to the management portal for their tenant. Common uses include providing an on-site employee access to reset peers' passwords, assign application or allow manual server wakeup access. Permissions controlling what areas of the console can be seen is set here as well.

Logoff user(s)

Logged on users can be logged off by the VDS admin from the Users/Groups page in VDS.

Applications

Displays the application deployed in this workspace. The check box provisions the apps to this specific user. Complete Application Management documentation can be found here. Access to applications can also be granted from the App interface or to Security Groups.

View/kill user processes

Displays the processes currently running in that user's session. Processes can be ended from this interface as well.