



Training Guide

PASSWORD CONTROL



E: help@avinet.com.au

W: avinet.com.au

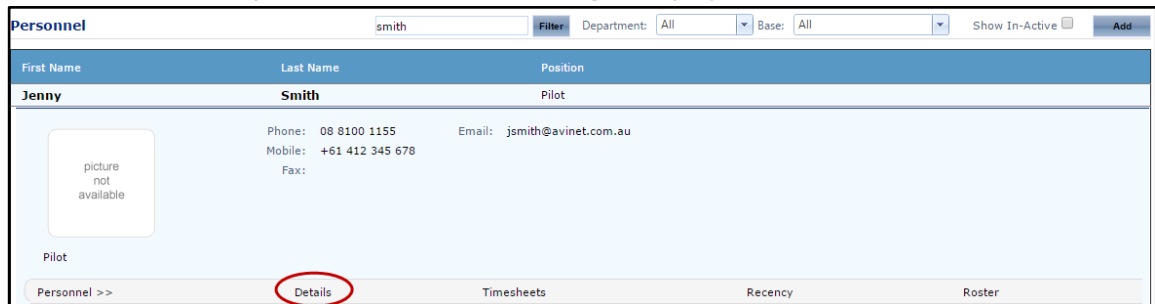
Contents

- Assigning Access Levels 3
- Setting Up Password Controls 4
- Unlocking User Accounts 5

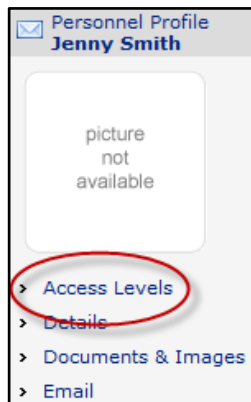
Assigning Access Levels

Before users can attempt to manage passwords, they must be assigned the correct access levels. Follow the steps below to assign the access levels:

- Step 1. Select **Operations > People > Personnel**. The **Personnel** screen is displayed.
- Step 2. Filter the **Personnel** screen according to your requirements.
 - Enter filter criteria in the text-box and click [Filter].
 - Select a value from the **Department** drop-down list to view personnel located in a particular department.
 - Select a value from the **Base** drop-down list to view personnel located in a particular base location.
 - Select the **Show In-Active** tick box to include personnel that are no longer active in the system. This includes personnel which have ceased employment with your organisation.
- Step 3. Click [Details] to view detailed personnel information. If you do not have the required access level to view personnel details, a warning is displayed.



- Step 4. Select 'Access Levels' from the **Personnel Profile** pane.



- Step 5. Click [Edit].
- Step 6. Select the **Personnel Management > Password Administration > Modify All** tick box.
- Step 7. Click [OK].

Setting Up Password Controls

Air Maestro's password control feature allows organisations to setup rules regarding user password requirements.

- Step 1. Select **Manage > Setup > Personnel**. The **Personnel Setup** screen is displayed.
- Step 2. Select the applicable password options in the **Password Complexity Requirements** (for non-LDAP accounts) pane.

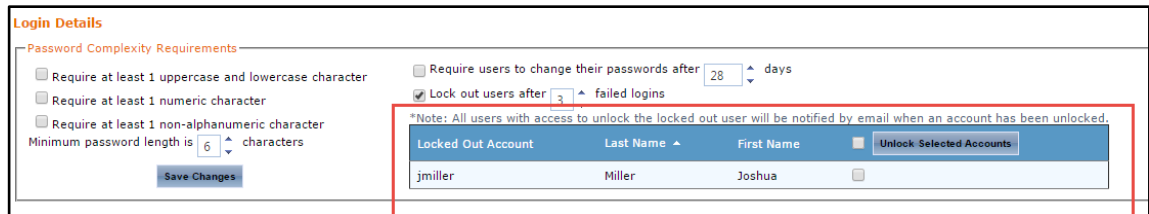
Wizard Stage	Description
Require at least 1 uppercase and lowercase character	Select whether passwords need to contain at least 1 uppercase and lowercase character.
Require at least 1 numeric character	Select whether passwords need to contain at least 1 numeric character.
Require at least 1 non-alphanumeric character	Select whether passwords need to contain at least 1 alphanumeric character.
Minimum password length is X characters	Enter the minimum characters required for passwords.
Require users to change their passwords after X days	Enter the number of days passwords remain valid. After the days elapse, users are prompted to change their password and the system does not allow them to proceed until they do so.
Lock out users after X failed logins	Enter the number of permitted invalid login attempts before system lock out.

- Step 3. Click [Save Changes].

Unlocking User Accounts

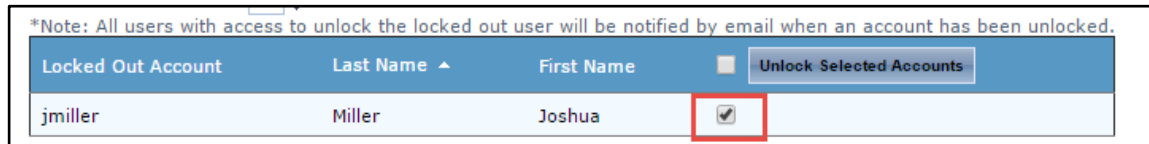
Air Maestro's lock out feature, prevents users from logging into Air Maestro after a specified number of failed login attempts. When users are locked out from their account, authorized personnel are required to unlock the account using the **Personnel Setup** screen.

Step 1. Select **Manage > Setup > Personnel**. The **Personnel Setup** screen is displayed. Locked out users are listed in the **Locked Out Account** pane.



The screenshot shows the 'Login Details' section of the Personnel Setup screen. Under 'Password Complexity Requirements', there are several options: 'Require at least 1 uppercase and lowercase character', 'Require at least 1 numeric character', and 'Require at least 1 non-alphanumeric character'. There are also input fields for 'Minimum password length is 6 characters' and 'Require users to change their passwords after 28 days'. A checkbox for 'Lock out users after 3 failed logins' is checked. A note states: '*Note: All users with access to unlock the locked out user will be notified by email when an account has been unlocked.' Below the note is a table with columns: 'Locked Out Account', 'Last Name', 'First Name', and an 'Unlock Selected Accounts' button. The table contains one row: 'jmiller', 'Miller', 'Joshua', and an unchecked checkbox.

Step 2. Select the tick box corresponding with the required locked out account.



This is a close-up of the table from the previous screenshot. The checkbox for the user 'jmiller' is now checked. The note above the table remains the same.

Step 3. Click [Unlock Selected Accounts]. The screen is refreshed and the user's account is unlocked.