Reference Guide

Administration

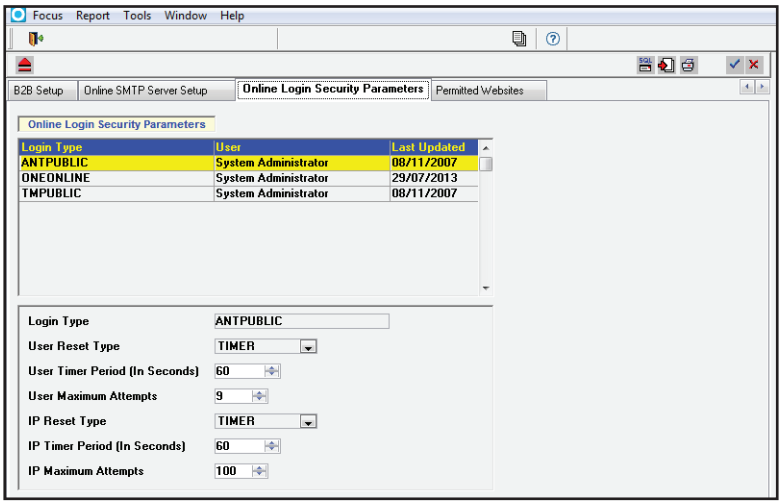
Hardening Guide

There are a number of hardening processes that should be undertaken in order to ensure One is as secure as possible. By setting appropriate lockout values, using suitable password complexity rules, and limiting the types of file that can be uploaded as linked documents, you can minimise the risk of unauthorised system access and data loss.

Configuring Login Security

One can be configured to lock user accounts after a certain number of unsuccessful attempts to log in to a given account. One can also block login requests from a specific IP address if that address sends a certain number of unsuccessful login attempts. If an IP address is blocked then no account can log in from that address, regardless of which user account made the failed attempts. You can set separate user and IP related lockout options for AnT Online public facing, Training Manager public facing and One v4 Online accounts.

1. Open the One v3 Client and select **Tools | System Administration** to display system-related options.
2. Select the **Online Login Security Parameters** tab to display editable fields relating to online security.



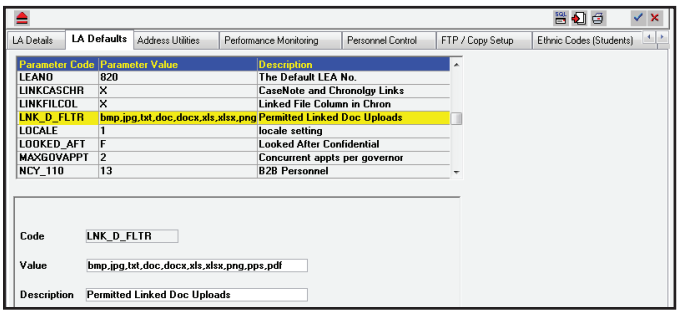
3. Select the **Login Type** whose options you wish to edit from the list. You can select from three login types:
   - **ANTPUBLIC** - Used for A&T Online (Public Facing) and the Citizen Self Service Portal.
   - **ONEONLINE** - Used for One v3 Online.
   - **TMPUBLIC** - Used for Training Manager (Public Facing).
4. Select the options for the user and IP related lockout options.
   - **Login Type:** The selected login.
   - **User Reset Type:** *Recommended setting: MANUAL.*
     If MANUAL is selected, a One Administrator must manually reset any locked-out user accounts. If TIMER is selected, the account automatically unlocks after the time specified in the **User Timer Period (In Seconds)** field has elapsed.
   - **User Timer Period (In Seconds):** *Range: 3-99999.*
     The wait period before an account unlocks automatically. After exceeding the **User Maximum Attempts**, the user cannot attempt another login until this time period has expired. The user must wait for the **User Timer Period** to expire after every subsequent unsuccessful login, until they log in successfully.
   - **User Maximum Attempts:** *Range: 1-999. Recommended setting: 4.*
     The maximum number of times that a user can attempt to log in before the account is locked out.
   - **IP Reset Type:** This option is always set to TIMER, meaning that IPs are automatically unblocked after the time specified in the **IP Timer Period (In Seconds)** field.
   - **IP Timer Period (In Seconds):** *Range: 3-99999. Recommended setting: 120.*
     The wait period before an IP is automatically unblocked. After exceeding the **IP Maximum Attempts**, the user cannot attempt another login from the blocked IP until this time period has expired. The user must wait for the **IP Timer Period** to expire after every subsequent unsuccessful login, until they log in successfully.
   - **IP Maximum Attempts:** *Range: 1-999. Recommended setting: 5.*
     The maximum number of unsuccessful logins that can be sent from a specific IP before that IP is blocked.
5. Click the check button to save your changes.

Administration
Hardening Guide

Configuring Allowed File Types

For security reasons, One restricts the file types that can be uploaded as linked documents. By default, only .BMP, .DOC, .DOCX, .JPG, .PNG, .PDF, .PPS, .TXT, .XLS and .XLSX files can be uploaded. To edit the allowed file type list:

1. In the v3 Client, select **Tools | System Administration | LA Defaults** to display the **Parameter Code** list.
2. Select the **LNK_D_FLTR** parameter code to display editable fields related to the allowed files list.
3. Enter the file extensions you wish to use into the **Value** field, separated by commas and without a full stop prefix. For example, if you only wanted One to accept .DOC, .PDF and .XLS files, you would enter “doc,pdf,xls”.
4. Click the check button to save your changes.

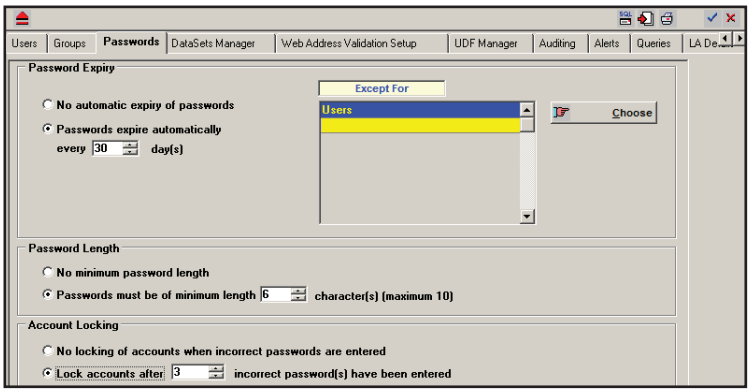


IMPORTANT NOTE: The default file list is deliberately kept short, in order to reduce the risk of malicious files being uploaded. It is strongly recommended that you do not add .ZIP or .EXE files to the list.

The list only applies to new uploads. All existing documents can still be downloaded. However, if the file type is not on the list then you cannot re-upload the document. For example, you could still download a previously-uploaded .ZIP file, but could not alter the contents of that file and then upload it again (assuming that .ZIP had not been added to the list of allowed file types).

Updating Password Rules

One’s password configuration options can be found on the v3 Client’s **Tools | System Administration | Passwords** tab. These options enable you to specify an expiry period, minimum length and maximum number of incorrect login attempts for account passwords.



Password Expiry Period

By default, **Password Expiry** is set to **No automatic expiry of passwords**. To set a password expiry period:

1. Select the **Passwords expire automatically** radio button to display options relating to password expiry.
2. Enter an expiry period (in days) into the **Passwords expire automatically** field.

NOTE: If the expiry limit is changed to *nn*, all user passwords (except those for whom an exception has been made) will expire *nn* calendar days after their last change of password. If any users have not previously changed their password, their password will expire *nn* calendar days after their next login.

3. Optionally, click the **Choose** button on the **Except For** panel to select users whose passwords should never expire.
4. Click the check button to save your changes.

Minimum Password Length

By default, **Password Length** is set to **No minimum password length**. To specify a minimum password length:

1. Select the **Passwords must be of minimum length** radio button to display the minimum length selector.
2. Enter a minimum number of password characters. It is recommended that this value is set to 8. The maximum is 10.
3. Click the check button to save your changes.

Administration
Hardening Guide

Updating Password Rules

Account Locking

By default, **Account Locking** is set to **No locking of accounts when incorrect passwords are entered**. To specify a maximum number of failed attempts before account lockout:

1. Select the **Lock accounts after a number of incorrect passwords have been entered** radio button and click **OK** on the pop-up message to display the number of attempts selector.
2. Enter the maximum number of attempts before lockout, up to 100. It is recommended that you set this value to 3.
3. Click the check button to save your changes.

NOTE: If a user exceeds the maximum number of logins in the A&T public facing application, a time lock of 20 minutes is applied.

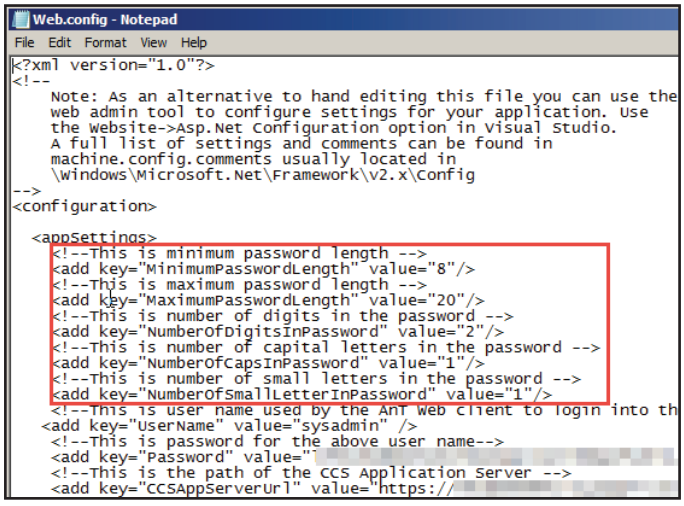
Passwords are created by the System Administrator in v3 Client. If you enable account locking, you should create an alternative System Administrator level account, with a non-standard user name, in case the default SYSADMIN account becomes locked.

Configuring Public User Password Complexity

You can use the parameters in the A&T web.config file to specify password complexity rules for public users. By requiring users to use a particular combination of digits, capitals and lowercase letters in their passwords, you can help to reduce the risk of data loss due to a brute force or guessing attack.

To specify password complexity rules:

1. Navigate to the **CCSAdmissionsOnline** folder in your test environment. The default location for this folder is *C:\inetpub\wwwroot\CCSAdmissionsOnline*.
2. Open the web.config file in Notepad.
3. Scroll to the **Configuration | AppSettings** section of the file and edit the password complexity key values as required. There are five settings you can configure:
   - **Minimum Password Length**
   - **Maximum Password Length**
   - **Number of Digits in the Password**
   - **Number of Capitals in the Password**
   - **Number of Small Letters in the Password.**
4. Save the file to confirm your changes.



NOTE: The default **Minimum Password Length** is six characters, while the default **Maximum Password Length** is 20 characters. The **Maximum Password Length** and the **Number of Digits in the Password** cannot be set to more than 30 characters.

CAPITA

Capita One. Tel: 01234 838080. Email: info@capita-one.co.uk. Web: www.capita-one.co.uk.