iLaps V2 maintance is only required with AAD Secrets, SAS Tokens Policy, and Admin UI SAS tokens expire

IF YOU WANT TO INVALIDATE ALL KEYS THEN READ SECTION AT END OF DOC

AAD Secret Expiration

By default Azure recommends Client Secrets to expire after 6 months, however you can choose to set them to 2 years or `custom` and set them to never expire.

1. Navigate to `Azure Active Directory`
2. Then `App Registrations`
3. Search for and select `ILAPS`
4. Click `Certificates & Secrets`
5. View the secrets at the bottom of the panel and check expiration date, if expiration is coming soon then create a new secret, copy the value.
    1. Navigate to Resource Group which `ilaps` is deployed via Azure Portal
    2. Find and open the web application in the Portal
    3. Click `Configuration`
    4. Search for `ClientSecret`
    5. Update the value then click `OK`
    6. Click `Save` this will cause the application to restart (recommend doing in maintence window)
6. Do not forget to update `settings.production.local.json` file also so subsequent builds are successful and work when debugging locally

Install Script Blob Storage Key

Locate `output/Install-iLaps_v2.0.ps1` and `$AzureSharedAccessSignature` variable and see when expiration is set in the string (`se=DATE`). If you do not have the output folder check `settings.production.local.json`. If expiration is close follow steps below to create new secrets.

Navigate to iLAPs storage account via Azure Portal

1. Create Shared Access Signature for `Installation Script`
    1. Allowed Services: Blob
    2. Allowed Resource Types: Object
    3. Allowed Permissions: Read
    4. Set Start and End Expiration dates
    5. Allowed Protocols: Https only
    6. Generate SAS and Connection String
    7. Save into `settings.production.local.json` field shown below

```
    "Blob-Object-Read-Installer-SAS-Token": "PasteValueHere"
```

2. After you have updated the secret run `build.ps1` again and check `output/Install-iLaps_v2.0.ps1` and push via intune (instructions in Readme if you need them again)

Admin User Interface Secrets

Using Azure Portal:

1. Navigate to Resource Group which `ilaps` is deployed via Azure Portal
    1. Find and open the web application in the Portal
    2. Click `Configuration`
    3. Search for `SASToken`
    4. Check `se=DATE` and see if date is about to expire soon, If so follow below
2. Navigate to iLAPs storage account via Azure Portal
    1. Create Shared Access Signature for `Admin UI`
        1. Allowed Services: Table
        2. Allowed Resource Types: Object
        3. Allowed Permissions: Read, Write, List, Add, Create, Update
        4. Set Start and End Expiration dates
        5. Allowed Protocols: Https only
        6. Generate SAS and Connection String
        7. Save into `settings.production.local.json` field shown below

```
    "Admin-UI-Table-Object-Read-Write-List-Add-Create-Update-SAS-
Token": "PasteValueHere"
```

3. Go back to step `1.3` and update using SAS Token from `2.1.6`

Reset and Check Reset Script Policy

1. Navigate to Storage account via Azure Portal
2. Click `Tables` click the elipsis on `AdminPassword` table
    1. Select Access Policy
    2. Click Edit on `Add-Create`
    3. Update Start/Expiry
    4. Click Ok

5. Click Save

3. Click `Tables` click the elipsis on `ResetPasswords` table

    1. Select Access Policy
    2. Click Edit on `Read-Update`
    3. Update Start/Expiry
    4. Click Ok
    5. Click Save

4. If you chose to roll the primary keys, then you will need to also rebuild all scripts and push them to storage account again along with update intune install script to force script reinstallation with new keys

IF YOU WANT TO INVALIDATE ALL KEYS THEN NAVIGATE TO PORTAL > STORAGE ACCOUNT > ACCESS KEYS > CLICK THE REFRESH NEXT TO KEY1 AND KEY2

IF YOU CHOSE TO RESET KEYS YOU WILL NEED TO DO THE FOLLOWING AGAIN AND RERUN THE BUILD.PS1

13. Open `Azure Storage Explorer`

    1. Login to Azure and find the storage account we just created

    2. Open the `Tables` section

    3. Right Click `AdminPasswords` table

        1. Click `Get Shared Access Signature...`

        2. Click `Access Policy` and select `Add-Create`

        3. Click Create

        4. Copy the `Query String`

            1. Save into `settings.production.local.json` field named

```
"Table-Object-Add-Create-SAS-Token": "PasteValueHere"
```

        5. Click `Back` and change the `Access Policy` to `Read`

        6. Click Next

        7. Copy the `Query String`

            1. Save into `settings.production.local.json` field named

```
"Table-Object-Read-List-SAS-Token": "PasteValueHere"
```

4. Right Click `Reset Passwords` table
    1. Click `Get Shared Access Signature...`
    2. Click `Access Policy` and select `Read-Update`
    3. Click Create
    4. Copy the `Query String`
        1. Save into `settings.production.local.json` field named

```
"Table-Object-Read-Update-SAS-Token": "PasteValueHere"
```