Knowledge article

Intune Management with Broker2.0

Created 4 months ago Active 3 months ago Last edited 3 months ago Viewed 342 times 5 min read

msal-linux linux-desktops See all editors

Share article ••• Edit article

4

8

Configuring Linux Desktop

This article provides instructions for configuring your Linux Desktop to enroll in Intune management, enabling you to access M365/Azure resources secured by Conditional Access via the Edge Browser with a logged-in Edge Profile.

Please re-visit this page for the latest up-to-date information regarding this pilot.

Bugs can be submitted via: https://aka.ms/oneauthbug

The query for Broker2.0 related bugs is here: Justin-linux-Broker2.0-Bugs

NOTE: We have only tested Ubuntu 22.04 and 24.04 at this time. RHEL support will come after we stabilize ubuntu.

Broker2.0 Change Log

2.0.2 release

- 9/19 - Added Telemetry to the header of token requests so we can differentiate broker versions.
- Currently there is no migration script to migrate state from the javabroker to broker2.0. To test the new broker, you will need to remove the javabroker and all state, and re-register your device via intune + broker2.0.
- When onboarding a new device, the device will perform an Entra Join instead of an Entra Registration. This means it is a device trust, instead of a registration within the user profile. This is a prerequisite step to enable platformSSO in the future.
- Renamed the device broker service from `microsoft-identity-device-broker` to `microsoft-identity-devicebroker`
- There no longer is a user broker service named `microsoft-identity-broker`. The user broker is now an executable that gets invoked via dbus connection
- Device certs are moved from the Keychain to `/etc/ssl/private`. In that directory, there will be a device cert per tenant, a session transport key per tenant, and a deviceless key that is stored in that directory. All other user data such as AT/RT are stored in the KeyChain and accessed via msal/OneAuth.

New Install

This article provides instructions for configuring your Linux Desktop to enroll in Intune management, enabling you to access M365/Azure resources secured by Conditional Access via the Edge Browser with a logged-in Edge Profile. This assumes that you have removed the previous Javabroker (version 2.0.1 or <). If you need to clean up the javabroker install, please see the section "Removing components" below that documents the known set of steps to fully remove the broker and any reminents.

Step 1 - Add the apt sources & install for Edge and Intune

```
# Install Curl
sudo apt install curl

# Install Microsoft's public key
curl https://packages.microsoft.com/keys/microsoft.asc | gpg --dearmor >
microsoft.gpg
sudo install -o root -g root -m 644 microsoft.gpg /usr/share/keyrings
rm microsoft.gpg

# Install the production packages:
sudo sh -c 'echo "deb [arch=amd64 signed-by=/usr/share/keyrings/microsoft.gpg]
https://packages.microsoft.com/ubuntu/$(lsb_release -rs)/prod $(lsb_release -cs)
main" >> /etc/apt/sources.list.d/microsoft-ubuntu-$(lsb_release -cs)-prod.list'
```

```
wget "https://packages.microsoft.com/config/ubuntu/$(lsb_release -rs)/insiders-fast.list" > /etc/apt/sources.list.d/microsoft-insiders-fast.list
sudo apt update

# Install Edge's dev channel repo
sudo sh -c 'echo "deb [arch=amd64] https://packages.microsoft.com/repos/edge stable main" > /etc/apt/sources.list.d/microsoft-edge-stable.list'

sudo apt update

# Install Edge
sudo apt install microsoft-edge-stable

# Install Microsoft Edge - IMPORTANT! You need to install the broker first
sudo apt install microsoft-identity-broker

# Install Intune
sudo apt install intune-portal

# List installed packages & versions
sudo dpkg -l microsoft-identity-broker intune-portal microsoft-edge-stable azure-cli

#  ========================================================
# Install Smart Card drivers
# Set up YubiKey
  sudo apt install pcscd yubikey-manager

#Yubikey/Edge Bridge
  sudo apt install opensc libnss3-tools openssl
  mkdir -p $HOME/.pki/nssdb
  chmod 700 $HOME/.pki
  chmod 700 $HOME/.pki/nssdb
  modutil -force -create -dbdir sql:$HOME/.pki/nssdb
  modutil -force -dbdir sql:$HOME/.pki/nssdb -add 'SC Module' -libfile /usr/lib/x86_64-linux-gnu/pkcs11/opensc-pkcs11.so
```

Step 2 - Login & Configure Intune

Once everything is installed & configured per the previous steps, you'll want to launch Intune (Company Portal) to login & register/enroll your desktop in Intune management.

Log-in with your USER@Microsoft.com credentials, and enroll your desktop. Once this step completes, you should end up with a page in the Intune Agent telling you that your desktop is either compliant or not (with steps to mitigate). If your desktop is found compliant, you can close intune if you'd like, and you should see your device on the portal dashboard.

> When troubleshooting, it is best to launch from the command line, as you'll get stdout for any errors or such, but you can equivalently launch "Company Portal" from applications manually if you'd like.

```
# Run Intune-Portal
# open second terminal window
/usr/bin/intune-portal

cd /opt/microsoft/intune/bin
INTUNE_LOG_LEVEL=debug ./intune-portal
```

Step 3 - Run Edge

Once you've configured intune, you'll now want to access your M365 resources! Currently, the only way you'll be able to access M365 resources is using Edge Browser - we do not currently support CA for Ubunutu for M365 using anything else but Edge.

The first steps is to launch edge. Simply open the Edge dev shortcut from the launcher, or execute the following from the terminal:

```
microsoft-edge
```

This should launch edge. It is also worth noting that you must login to the Edge Profile to be able to use this integration. If you aren't prompted to create a new profile, you can find the grey person icon in the top right corner of edge - simply click on the image and select **"Sign in to sync data"**. You'll want to enter your USER@Microsoft.com account, and this should provide SSO to login to other sites such as office.com.

OPTIONAL - To install Azure CLI

Reference

```
# All in One Command:
curl -sL https://aka.ms/InstallAzureCLIDeb | sudo bash

# Step by Step
sudo apt-get update
sudo apt-get install ca-certificates curl apt-transport-https lsb-release gnupg
curl -sL https://packages.microsoft.com/keys/microsoft.asc |     gpg --dearmor |
sudo tee /etc/apt/trusted.gpg.d/microsoft.gpg > /dev/null
AZ_REPO=$(lsb_release -cs)
echo "deb [arch=amd64] https://packages.microsoft.com/repos/azure-cli/ $AZ_REPO
main" |     sudo tee /etc/apt/sources.list.d/azure-cli.list
sudo apt-get update
sudo apt-get install azure-cli
az -v
```

Update to latest packages

Run the following

```
# Update package/repo metadata
sudo apt update

# upgrade packages & clean up dependencies
sudo apt-get dist-upgrade
```

List installed versions

To list the package versions currently installed, run: (Reference)

```
apt list -a intune-portal microsoft-edge-dev microsoft-identity-broker azure-cli
#or
sudo dpkg -l microsoft-identity-broker intune-portal microsoft-edge-stable
```

PRMFA testing:

To install the SmartCard services:

```
# https://p11-glue.github.io/p11-glue/p11-kit/manual/pkcs11-conf.html
module: /usr/lib/x86_64-linux-gnu/libykcs11.so
```

The following lists several steps of configuring Yubikey/Edge bridge

```
# Set up YubiKey
  sudo apt install pcscd yubikey-manager

#Yubikey/Edge Bridge
  sudo apt install opensc libnss3-tools openssl
  mkdir -p $HOME/.pki/nssdb
  chmod 700 $HOME/.pki
  chmod 700 $HOME/.pki/nssdb
  modutil -force -create -dbdir sql:$HOME/.pki/nssdb
  modutil -force -dbdir sql:$HOME/.pki/nssdb -add 'SC Module' -libfile
/usr/lib/x86_64-linux-gnu/pkcs11/opensc-pkcs11.so
```

Removing components / Resetting configuration

If for some reason you need to manually reset & uninstall components, here are the settings required to clean up.

To Remove Intune & the identity broker

```
sudo apt remove microsoft-identity-broker
sudo apt remove intune-portal
```

To force remove broker2.0 device identity:

```
sudo rm /etc/ssl/private/drs*
sudo rm /etc/ssl/private/stk*
```

To clear out the keychain (MSAL & intune cache):

```
# remove secrets stored
secret-tool search --all env
60a144fbac31dfcf32034c112a615303b0e55ecad3a7aa61b7982557838908dc
secret-tool clear env
60a144fbac31dfcf32034c112a615303b0e55ecad3a7aa61b7982557838908dc

secret-tool search --all name LinuxBrokerRegularUserSecretKey --unlock
secret-tool search --all name LinuxBrokerSystemUserSecretKey --unlock
secret-tool clear name LinuxBrokerRegularUserSecretKey
secret-tool clear name LinuxBrokerSystemUserSecretKey
```

Full Scripts to force remove the config:

```
# uninstall the applications
sudo apt remove microsoft-identity-broker
sudo apt remove intune-portal

# Stop Identity Service
sudo systemctl stop microsoft-identity-devicebroker

# Clean up service state
sudo systemctl clean --what=configuration --what=runtime --what=all microsoft-
identity-devicebroker.service

# Clear device keys
sudo rm /etc/ssl/private/drs*
sudo rm /etc/ssl/private/stk*

# Clear file chaches
sudo rm -r "$USER_HOME/.cache/microsoft-identity-broker"
```

```
sudo rm -r "$USER_HOME/.config/microsoft-identity-broker"
sudo rm -r "$USER_HOME/.local/share/microsoft-identity-broker"
sudo rm -r "$USER_HOME/.local/share/intune"
sudo rm -r "$USER_HOME/.config/intune/registration.toml"
sudo rm -r "$USER_HOME/.local/share/intune-portal"
sudo rm -r "$USER_HOME/.cache/intune-portal"
sudo rm -r "$USER_HOME/.local/share/intune-portal"
sudo rm -r "$USER_HOME/.config/intune"

# Clear intune config
rm -r ~/.config/intune

# Optional, but this can potentially free space by some larger dependencies that
the auth broker require
sudo dnf autoremove

# remove secrets stored
secret-tool search --all env
60a144fbac31dfcf32034c112a615303b0e55ecad3a7aa61b7982557838908dc
secret-tool clear env
60a144fbac31dfcf32034c112a615303b0e55ecad3a7aa61b7982557838908dc

secret-tool search --all name LinuxBrokerRegularUserSecretKey --unlock
secret-tool search --all name LinuxBrokerSystemUserSecretKey --unlock
secret-tool clear name LinuxBrokerRegularUserSecretKey
secret-tool clear name LinuxBrokerSystemUserSecretKey

# Verify device is removed from Company Portal
#    - On a managed device browse to https://aka.ms/cpweb
#    - Click Devices
#    - locate the Linux device, and if it is there select it
#    - Click Remove
```

Troubleshooting & Reporting Issues:

Bugs can be submitted via: https://aka.ms/oneauthbug

The query for Broker2.0 related bugs is here: Justin-linux-Broker2.0-Bugs

Logging

Item	Command
All Logs	`journalctl --since "10 minutes ago" > logs_last_10_min.txt`
Intune	`journalctl -f --user -u intune-agent` `journalctl -f --user -t intune-portal > intune-portal.log`
JavaBroker	`journalctl --user -f -u microsoft-identity-broker.service` `sudo journalctl --system -f -u microsoft-identity-device-broker.service`

Item	Command
New Broker	`journalctl --user -f -u microsoft-identity-broker.service`
DBUS Logs	`busctl --user monitor com.microsoft.identity.broker1`

Services

Services:	
To get All running services:	`systemctl --type=service --state=running`
Restart Broker2.0	`sudo systemctl --user restart microsoft-identitybroker.service`
Get status of Javabroker	`systemctl --user status microsoft-identity-broker.service`

Get installed apps & Versions:

```
sudo dpkg -l microsoft-identity-broker intune-portal microsoft-edge-stable azure-cli
```

Run intune w/ debug level

```
cd /opt/microsoft/intune/bin
INTUNE_LOG_LEVEL=debug ./intune-portal
```

To get what versions are installed

How To/Why articles:

- How do I find out my Intune DeviceId
- How do I capture the broker logs?
- List all the versions of components installed for registering my Linux Desktop in AAD & Intune
- How to reset my Linux desktop from Enrollment in Intune

- On Linux Desktops, how do I safely update/upgrade to the latest Intune Agent?
- Why does the user get a "Are you trying to sign into the Microsoft Authentication Broker" prompt during Linux Desktop Enrollment?
- What does "reset ... to factory setting" actually mean?

edited Sep 26 at 20:22

created Aug 23 at 0:32

Justin Ploegert

542 2 11

If you hit a black screen add this ENV `WEBKIT_DISABLE_DMABUF_RENDERER=1 intune-portal` – Youssef Shahin Nov 4 at 21:35