Devices

Overview

Create and manage Local and Remote Device records and corresponding Company and People associations, as well as static Device Groups

Devices are the “target” of filter settings configured in **Content Filter**.

Note: for proper network operation:

- all Devices need to have the DrawBridge CA Security Certificate installed. See **Essential Concepts: Web Page Classification: Traffic Visibility Prerequisites** for further information.
- Remote Devices must have the correct External Networks assigned to them. See page **Remote Devices** in this chapter for further information.

Identifying Devices on the network

The DrawBridge has several ways of identifying Devices

- Local Devices via either
  - auto-created records via built-in network detection, or,
  - auto-created records via the DrawBridge Agent software (Windows-only), or,
  - manually created records by a user.
- Remote devices created by users; these authenticate with the DrawBridge username and password

In this chapter:

- Devices Dashboard
  - Local Devices
  - Remote Devices
  - Device Groups
- Apps: Device Configuration
  - SSL Certificates
  - External Networks

Devices Dashboard

- **Local Devices:** devices on the network where your DrawBridge is located.

For example, the desktop you have in your office.

- **Remote Devices:** devices that access your DrawBridge from “outside” your network; ie. from the public Internet.
  For example, a laptop that’s configured to connect to your DrawBridge for filtering whenever you’re out on the road using a hotspot.
- **Device Groups:** entities that contain Local and/or Remote devices

Apps: Device Configuration

- **SSL Certificates:** mandatory SSL/TLS Certificate Authority security certificates for all devices connecting through a DrawBridge
- **External Networks:** list of external network information used for assisting Remote Device Authentication operations

Local Devices

A Local Device record is an an entity intended to represent one Device on the local network, no matter how many network interfaces the Device has. (Exception: special IP Range devices; see FAQ below)

Devices are created by:

- **Auto-detection:** The DrawBridge monitors network traffic to detect local devices based on the IP address, and automatically creates a Local Device record if none exists for that address.
- **A DrawBridge Console user:** Click the **+** located in the upper right corner of the Local Devices list view to to create a new Local Device Record.
- **The DrawBridge Agent:** If the DrawBridge agent "calls home" with Device information that does not match an existing record, a new Local Device record will be created (*only* if the MAC address can be validated; see FAQ below)
- **Active Directory sync:** If your DrawBridge is configure to sync with an Active Directory server, Devices listed in the AD server will be automatically created on the DrawBridge.
- **Compass Portal Sync:** (Remote Devices Only)

In the Local Device list view, select any local device record by tapping the device name or IP address link shown in the `Hostname` column to see an individual device record.

Record View

A Local Device record contains the following parameters:

Parameter	About
Company	the Company associated with the Device; see **Accounts: Companies** for more information
Auto Hostname	the automatically-detected hostname of the device on the network, if available
Platform	the operating system of the device, if specified
Type	the type of hardware, such as Laptop, Smartphone, Tablet, and so forth
Status	this local device record is: `Active` or `Inactive`
Source	origin of the record information: auto-detected or User Entry

Parameter	About
Last Active	the timestamp of the last filter traffic recorded for this device
Reportable	traffic from this device Is or Is Not included in Activity Reports

Device Record header buttons:

- Add a new Local Device record with the blue **+** Create Local Device button
- Edit this Local Device record with the green pencil Update Local Device button
- Delete this Local Device record with the red trashcan Delete Local Device button
- Hamburger menu:
  - Today's Log Lines: a shortcut to the the *Reports* module with the device pre-selected in data views
  - Add Network Interface**: add an additional network interface to the device
  - Reset DrawBridge Agent: reset the record association with the DrawBridge Agent
  - Record Activity Stream: view the changelog for this Device record
- Bookmark this page with the ribbon Bookmark button

Informational Tabs

- **Network Interfaces**: IP address(es) and Mac address(es) associated with the device. Keep in mind that a device can have multiple network interfaces and also multiple IP addresses, so multiple lines may be listed here. For example, a laptop may have a Wi-Fi network interface as well as a wired Ethernet interface. Both interfaces will have unique MAC/hardware addresses, so if you want to apply a filter policy to that particular Device, no matter how it is connected to your network, you’ll need to ensure both interfaces (WiFi and Ethernet) are specified here.
- **Access Policies**: a list of Access Policies that are applied to this device. (see **Content Filter: Access Policies** for further information)
  This list is generated based on the membership of the Device in a particular *Device Group*, a component of an *Access Policy*. The exact Access Policy can be visited by clicking the link in the list under the Name column, or, you can view all Access Policies for your company by clicking the *Access Policies/Access Policy Dashboard* button to the right.

Device Group Membership

A local device is always part of the *alldevices* Device Group of the associated Company. A local device can be associated with an unlimited number of Device Groups. See the Device Groups page for further information

FAQs

Q: Why aren't Local Devices automatically appearing on my account?

A: Auto-generated Local Device records are only generated for the Main Company. Verify that your account is set as Main if you are not seeing Local Device records auto-populate.

Q: Why doesn't the Local Device record display the MAC address of my device?

A: Bogus/Randomized MAC addresses may be automatically discarded by the console to reduce the amount of auto-generated Local Device records. For more context and a resolution, see the Question "Why are there so many Local Devices listed?".

Q: Why are there so many Local Devices listed? (I only have X number of devices on my network.)

A: Several factors may result in a proliferation of Local Device records:

- **“Network churn”**: many new devices joining the network and old ones leaving. The DHCP server will do its job to utilize the limited address space available to it, which may involve assigning a previously-used address to a new device. This may result in the DrawBridge creating additional Local Device records or unexpectedly adding new MAC address associations to an existing IP Address / Hostname record.
  Countermeasure: configure address reservations in your network DHCP server (DrawBridge ClearOS webconfig panel or other network equipment, if applicable) to ensure that a specific MAC address may only ever be assigned a specific IP address.
- **Operating system privacy features**: randomized hardware interface addresses (also known as MAC addresses). Most operating systems now have functionality to generate a random hardware address for a particular network to prevent devices from being tracked across public WiFi hotspots. While most Operating Systems will maintain the same randomly-generated MAC address for a particular “remembered” network, if you reset your network settings or Forget the saved network, and re-join, the randomly-generated MAC will have changed. As above, this may result in the DrawBridge creating additional Local Device records or unexpectedly adding new MAC address associations to an existing IP Address / Hostname record.
  Countermeasures: Turn off physcial/MAC address randomization for your DrawBridge-protected network name (for example, for your WiFi network), and then set a DHCP reservation for the actual device hardware MAC address. Turn off hardware address randomization, by operating system:
  - iOS: Settings/WiFi/ information icon/ toggle `Private WiFi Address` off
  - Android: Settings/WiFi/ gear icon/Advanced/set `Privacy` to `Use Device MAC`
  - Windows 10; All Networks: Settings/Network and Internet/WiFi/toggle `Use random hardware addresses` off
  - Windows 10; Specific Network: Settings/Network and Internet/WiFi/Manage Known Networks/select /Properties/set `Use random hardware addresses` to off
  - Windows 11: Settings/Network and Internet/WiFi/ gear icon/Advanced/Privacy/set `Use device MAC`

  Then add an address reservation in your DHCP server, as described above.

> **Note:** The DrawBridge console does perform a background cleanup of "dead" local device records on a regular basis.

Q: Any type of "agent" software available for Windows computers to positively identify Local Devices on a network?

A: Yes! See the page **DrawBridge Agent Reference** in this chapter for further information

---

Q: Can I create an “entity” for an IP address range instead of making a bunch of Local Device records?

A: Yes! Create a new Local Device, and in the Platform field, select `Network IP / IP Range`, then enter the IP address range. This special “Local Device” can be used in a Device Group just like an ordinary Local Device or Remote Device record.

Remote Devices

A Remote Device connects through your DrawBridge from "outside" your network -- from the public Internet.

Remote Devices are created by:

- **A DrawBridge Console user:** Click the **+** located in the upper right corner of the Local Devices list view to to create a new Local Device Record.
- **CF Odoo Portal sync:** Devices created in the Portal are automatically synchronized either via a triggered sync run (Cloud Servers), or the scheduled sync job.

In the Remote Device list view, select any remote device record by tapping the username shown in the `Filter Username` column to see an individual device record.

Record View

The individual Remote Device record contains the following parameters:

Parameter	About
Company	the Company associated with the Device; see the Accounts section for more information
Console User	the Person record associated with the Remote Device
Filter Username	the unique username this Device uses for authentication; this must either ***match*** or ***begin with*** the username of the associated Console User/Person
Email	the email address of the associated Person record
Status	this device record is: `Active` or `Inactive`
Canonical ID	the global unique identifier for this Remote Device; used for synchronization
Contact CID	the global unique identifier of the associated Person record; used for sychronization
Last Active	the timestamp of the last filter traffic recorded for this device
Device Type	the type of hardware, such as Laptop, Smartphone, Tablet, and so forth

Remote Device Record header Buttons:

- **Add** a new Remote Device record with the blue **+** Create Remote Device button
- **Edit** this Remote Device record with the green pencil Update Remote Device button
- **Delete** this Remote Device record with the red trashcan Delete Remote Device button
- Hamburger menu:
  - **Update Personal Details:** edit the information of the associated Person record
  - **Set Console Password:** set a DrawBridge Console password for this Remote Device User
  - **Add Group Membership:** add this Remote Device User to a Console Permission Group (see Informational Tabs: Permissions, below)
  - **View Realtime Log Lines:** jump to the Realtime Log Viewer, with the data view limited to this device
  - **Today's Log Lines:** jump to the the *Reports* module with the device pre-selected in data views
  - **Record Activity Stream:** view the changelog for this Device record
- **Impersonate User** (take on the identity and permissions of this Remote Device user in the DrawBridge; used for troubleshooting)
- **Bookmark** this page with the ribbon Bookmark button
- Sync Menu (chain-link icon)
  - Sync Mode (default is `2 Way - Push / Pull from Server`); click record sync information
  - Push to Sync Publisher: initiate a record update push from this DrawBridge to the Sync Server
  - Pull from Sync Publisher: initiate a record update pull to this DrawBridge from the Sync Server
  - Mark to Resync: flag this record in the background to be included in the next sync run

Informational Tabs

- **Authentication**: Additional parameters used to identify the device to streamline authentication. See *Why do I need to have a Port/Platform/ExternalNetwork set for a Remote Device?* in the FAQ below.
  Also displayed are:
  - **User URL:** a link that can be visited in a browser on the device to authenticate its public IP with the DrawBridge
  - **PAC URL:** Proxy Auto-Configuration: a spec-compliant URL that can be used by major operating systems to programatically fetch proxy settings
- **Auth Activity**: A recent history view of public IP addresses that this device has successfully authenticated from, in addition to the associated reverse-DNS network name, when retreivable.
- **Access Policies**: a list of Access Policies that are applied to this device. (see Content Filter for more information on Access Policies) This list is generated based on the membership of the Device in a particular Device Group, a component of an Access Policy. The exact Access Policy can be visited by clicking the link in the list under the Name column, or, you can view all Access Policies for your company by clicking the Access Policies/Access Policy Dashboard button to the right.

- **Permissions**: a list of Console Permission Groups that this Remote Device User is a member of. (Permits or does Not Permit the submision of an AutoFix, for example)

Device Group Membership

A remote device is always part of the *alldevices* Device Group of the associated Company. A remote device can be associated with an unlimited number of Device Groups. See the Device Groups page for further information.

FAQs

Q: Why am I getting a `Proxy Authentication Required` popup on my mobile device?

A: Your device is not properly authenticated with the DrawBridge. Visit the **User URL** for your device in a browser on that device, and ensure you get a `Success` message.

If you continue to get these `Proxy Authentication Required` popups after a successful authentication event:

- Verify the proxy configuration on the device is correct (particularly the assigned port)
- Verify the network you are connecting from is listed in `External Networks` under the device. See the FAQ item below: *How does setting `Port`+`Platform`+`ExternalNetwork` information assist Remote Device authentication?*

Q: Why does the *Last Active* timestamp not line up with the known usage of the Remote Device?

A: This timestamp is the last recorded filter log activity for the device. There are several possibilities to explain why a device that is known to be in-use is not showing a current corresponding timestamp:

1. *The device does not have a data connection.*
   Solution:
   - Ensure the device has an active data plan and/or connect the device to an open WiFi network (not a captive-portal-controlled network, such as many public hotspots).
   - Perform activities on the device that will generate log data, such as visiting a search engine in a browser.
   - Verify while performing the activies that loglines are shown in the DrawBridge Realtime Log Viewer for the device.
   - If loglines for that device are displayed in the Realtime viewer, wait at least 15 minutes for the logs to be processed.
   - Refresh the Device Record page to see if the Last Active timestamp has been updated.

2. *The device is not properly authenticating with the DrawBridge, therefore, no web activity logs are being recorded.*
   Solution:
   - Follow the same steps as detailed above to verify there are loglines displayed in the Realtime Log Viewer for the device in question.
   - If there are no loglines, and yet web resources can be accessed on the device, then the proxy software on the device is failing to properly proxy traffic.
   - Verify the proxy settings/software on the device are correctly configured.
   - Visit the device User URL in a browser on the device to trigger an authentication event while monitoring the DrawBridge Realtime Log Viewer `Errors Log`, with the Remote Device port entered in the Pattern field. You should see one or more lines indicating successful authentication.

   Note for Android devices: Android has a "fail-open" proxy design, so if authentication fails for any reason, Android will bypass the proxy. This can generally be resolved by re-authenticating the device with the DrawBridge.
3. *The only traffic that is getting recorded is considered "system activity" and is not considered reportable, and is therefore not saved, so the* Last Activity *timestamp is not updated.*
   Solution: Follow the steps in #1 and #2 (if needed) to ensure the device is properly proxied and authenticating with the DrawBridge.

Q: Why do Remote Devices need to be authenticated?

A: It's critical for filtering and reporting purposes that the device that is connecting to the DrawBridge be postitively, unmistakably, identified.

Beyond that, anything connected to the internet is potentially a target for misuse. For example, if no authentication (username/password) was required for a remote device, a hacker could route their activities unimpeded through your internet connection, therefore making their malicious traffic appear to be originating with you. You may be held legally responsible for what happens on your internet connection. Depending on the type of activities, you may receive a legal notice warning of a DMCA violation. (Digital Millenium Copyright Act.) However, requiring authentication from all remote devices eliminates these concerns.

Q: How does setting `Port` + `Platform` + `ExternalNetwork` information assist Remote Device authentication?

A: As noted above, the DrawBridge requires authentication for Remote Devices. However, mobile operating system platforms (Android and iOS) are notorious for failing to always communicate the required credentials for authentication of each network session they establish. So, to smooth the user experience, the DrawBridge accomodates "assumed authentication" -- if a network request matches **all three** parameters:

- sent to the unique Port assigned to the device

- sent by the operating system Platform specified for the device
- originates from an External Network (mobile network) the device is known to be using

... then the DrawBridge will "assume" that the request is legitimate and consider the request authenticated. This prevents repeated `Proxy Authentication Required` popups on mobile devices as they roam cellular networks.

Device Groups

Device Group records are entities containing one or more Devices to which Access Policies can be applied. See **Content Filter: Web Page Access** for further information.

In the Device Groups list view, click the drop-down arrow button to the left of a line name to display member devices and associated Access Policies.

Depending on your Console Permission Group membership, and whether multiple Companies are present on your DrawBridge, you will be able to see all the Device Groups available on the system. See **Essential Concepts: Record Model - Tenancy and Hierarchy** for further information.

Note: This panel only displays "static" device groups. For parameter-based "Smart Device Groups", see the Content Filter module.

SSL Certs

The DrawBridge CA certificate is required on all client devices for proper operation with the DrawBridge.

Different operating systems require different certificate types or encoding types. This menu gives you the appropriate certificate for your operating system. Click the appropriate operating system for your use case and follow the instructions to install the certificate.

Visit the SSL Certs page

If you're on a DrawBridge-protected network, visit the SSL Certs dashboard at:

http://draw.bridge/sslcerts/dashboard/

If you're **not** on a DrawBridge-protected network, visit the SSL Certs dashboard on one of our cloud servers, such as:

- http://whitespire.compassfoundation.io/sslcerts/dashboard/
- http://sweetspire.compassfoundation.io/sslcerts/dashboard/

Linux systems

As of this writing, a script to install the DrawBridge root CA certificate is available on all DrawBridge systems, however it is not visible in the user interface at this time.

Installation instructions:

1. Download the installer script here: http://draw.bridge/static/software/linux_installer.zip (Note: must be on a DrawBridge-protected network with DNS resolution properly configured.)
2. Open a terminal and navigate to the directory where you saved the script. (eg. `cd ~/Downloads/`)
3. Extract the script: `unzip linux_installer.zip`
4. Run the script: `sudo ./Linux_Installer.sh`
5. Recommended: restart your system, or, at a minimum, your web browsers

External Networks

External Networks are used to assist with remote device authentication.

This list is managed by Compass and generally should not be edited. If you know of a new network that should be listed, please submit a support ticket to Compass (support@compassfoundation.io) to have the new External Network entry added to all DrawBridges.

DrawBridge Agent Reference

Overview

The DrawBridge Agent positively identifies and links the device it is installed on to a Local Device record in the DrawBridge. At initial install time, it will attempt auto-registration based on the device Hostname. Once the initial registration has occured, further authentication events identify the device to the DrawBridge using the registered Canonical ID (CID).

The DrawBridge Agent enables you to implement filter policies that follow a User around on your network, no matter what Device they are using, provided that the Windows User Name of the Person is known to the DrawBridge and matches a Person record present on the DrawBridge.

While this Agent was devloped primarily for companies with a Windows Active Directory server, it will also function on any local network that is protected by an onsite Drawbridge. Note that only Local Devices are supported (not Remote Devices, which presumably will be managed by a separate MDM [Mobile Device Management] service).

Notes regarding Active Directory Authentication Integration

See **Accounts: Authentication Integration** for more information on Active Directory server setup.

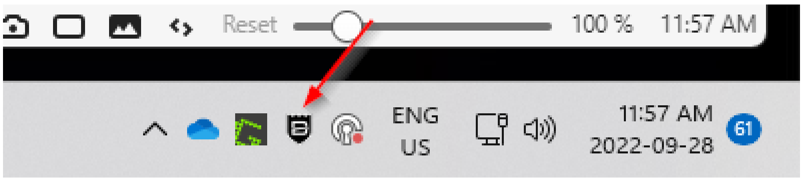
- After initial Active Directory (AD) sync configuration, People records and Group associations can be exclusively managed in the AD server, and the DrawBridge will automatically synchronize that information over.
  - The DrawBridge AD sync job automatically synchronizes over all Person and Directory Group records available in the AD infrastructure to the DrawBridge four times a day. (A manual sync can be triggered as well.)
- Directory Groups are entities pulled from an AD/LDAP server. A Directory Group must be designated as a Proxy User Group in the DrawBridge to be able to assign it to a Device Group for an Access Policy take effect on it.
  - See documentation book **How To Guides: Assign a Proxy User Group to an Access Policy** for further information.

Prerequisite Network Configuration

- `draw.bridge` must resolve to the local DrawBridge IP address on the local network. If the DrawBridge is not the DNS server, go to the network DNS server and create a new Forward Lookup Zone and create a new A record for `draw.bridge` to resolve it properly.

Agent Software Installation

- Download the latest version of the Drawbridge Agent installer from https://www.compassfoundation.io/drawbridge_agent/releases/drawbridge_agent.exe.
- Run the installer to install the Drawbridge Agent. By default it will be installed into the `C:\Program Files (x86)\Compass Foundation\DrawBridge Agent` folder. After a successful installation you should see an icon in the system tray.



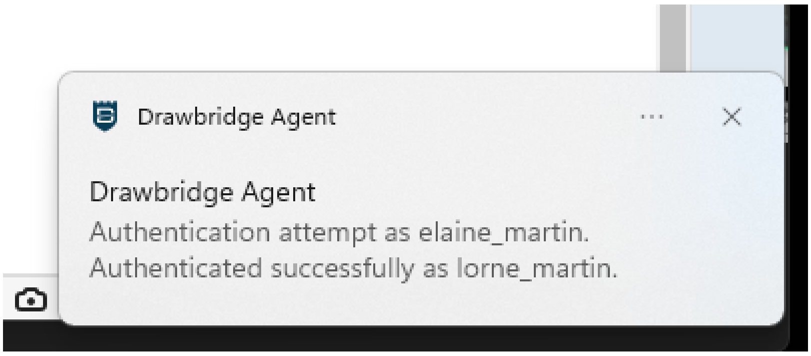
- It is also possible to run the installer silently with the following syntax.

```
DrawbridgeAgentInstallerX.X.Xexe /exenoui /qn
```

- A prerequsite to running the Agent is that the `.NET Desktop Runtime 6.0` or higher needs to be installed. The Drawbridge Agent installer will prompt the user to do this if it isn't already installed. In the case of a silent install, this will happen automatically if needed.
- Alternatively, the runtime can be manually downloaded and installed from Microsoft's Download Page.

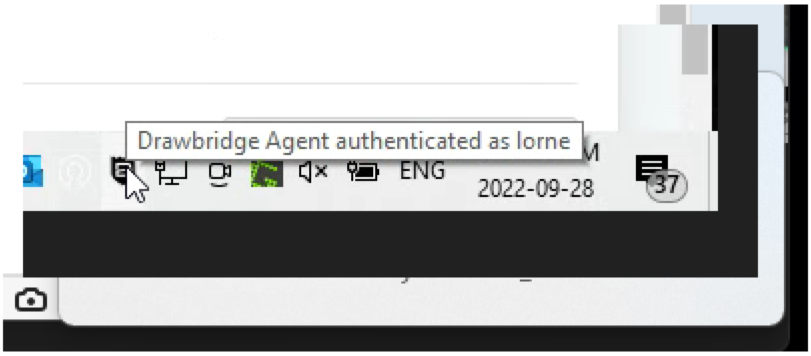
Operation

- After installation the user can click on the icon in the system tray. The Agent will first attempt to register with the Drawbridge by matching the device hostname with the hostname of a Local Device record in the DrawBridge, and if that is successful, it will attempt to authenticate with the Drawbridge.
- After this the Agent should automatically authenticate the currently logged in user at every Windows logon or unlock event. There will be toast messages shown to verify this, unless notifications are not turned on.

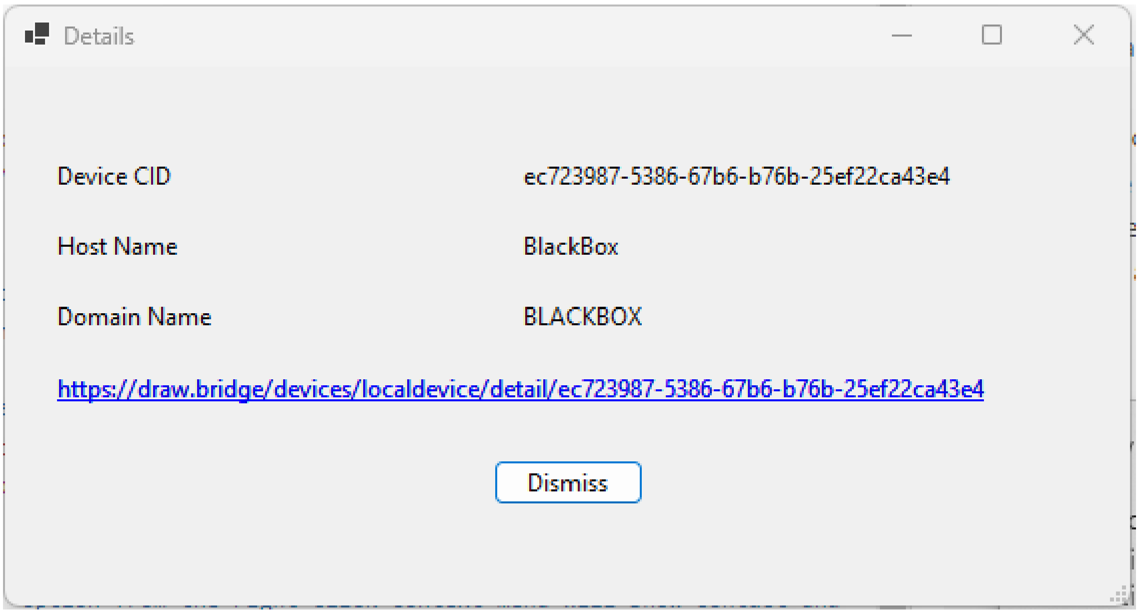


Drawbridge Agent
Authentication attempt as elaine_martin.
Authenticated successfully as lorne_martin.

- It is possible for the user to request a manual authentication with the Drawbridge. This is done either by left clicking on the icon in the system tray, or by right clicking and selecting `Authenticate User`.
- Hovering over the icon in the system tray will show the currently logged in Windows user name.


Drawbridge Agent authenticated as lorne

- Selecting the `About Version` option from the right click context menu will show contact and version information.
- Selecting the `More Info` option from the right click context menu will open a dialog with some additional info that may be useful for debugging.



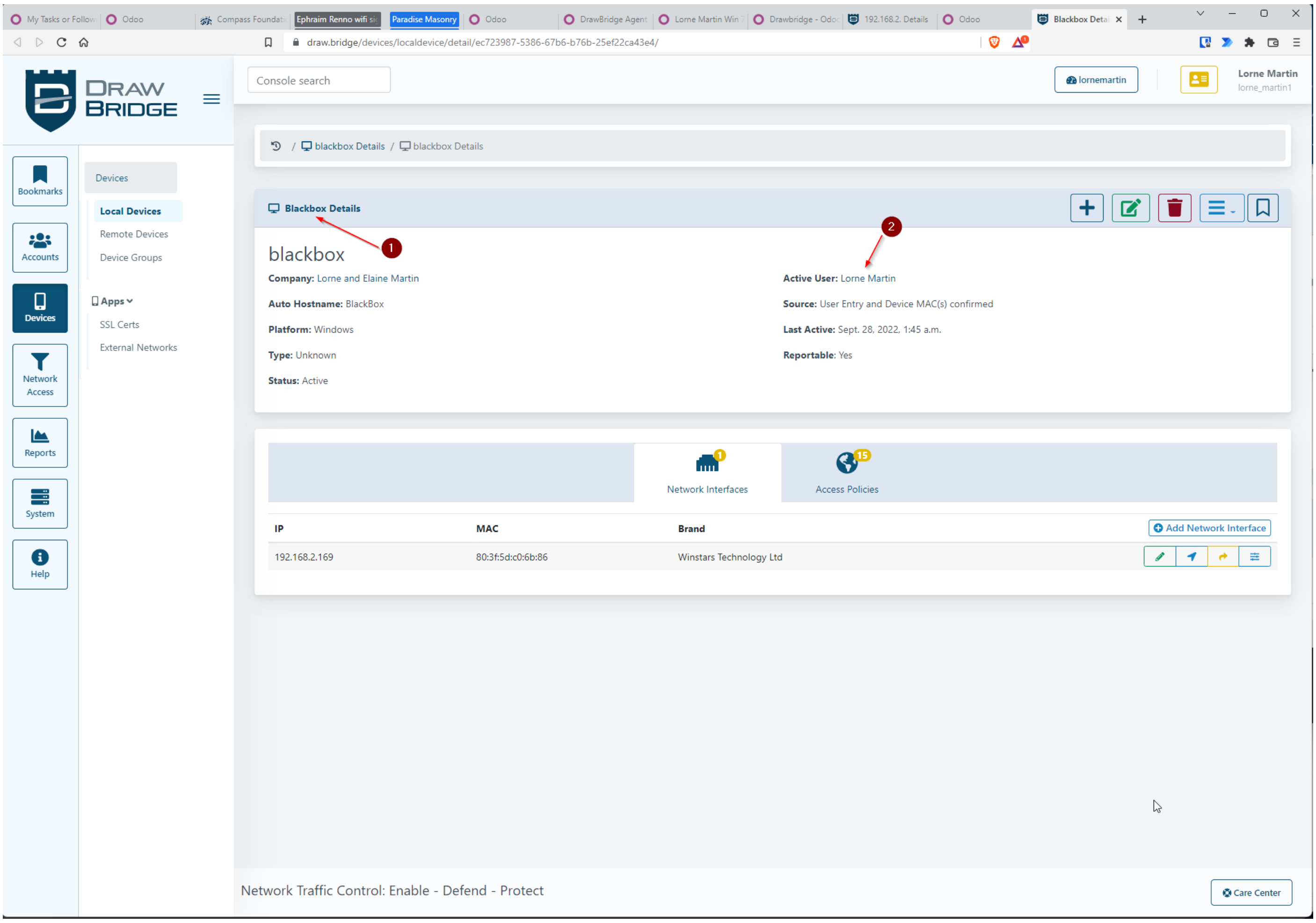
Device CID ec723987-5386-67b6-b76b-25ef22ca43e4

Host Name BlackBox

Domain Name BLACKBOX

https://draw.bridge/devices/localdevice/detail/ec723987-5386-67b6-b76b-25ef22ca43e4

- Clicking on the hyperlink in the details page will open up the console page for the local device that is currently being used. (#1 in screenshot). The console user that is currently associated with this device is shown at #2. This Active User can also be clicked on to open the console page for the user.



blackbox

Company: Lorne and Elaine Martin

Auto Hostname: BlackBox

Platform: Windows

Type: Unknown

Status: Active

Active User: Lorne Martin

Source: User Entry and Device MAC(s) confirmed

Last Active: Sept. 28, 2022, 1:45 a.m.

Reportable: Yes

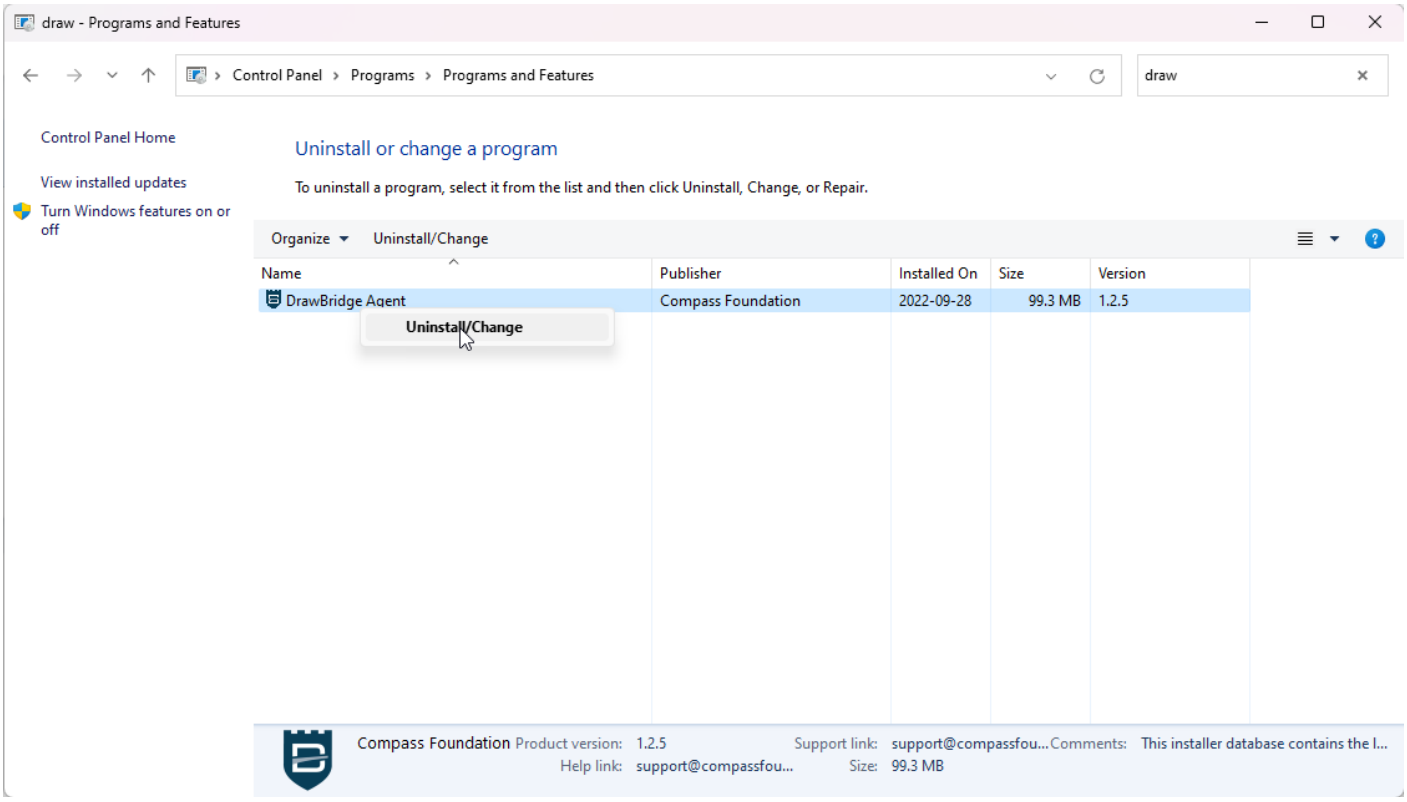
IP	MAC	Brand
192.168.2.169	80:3f:5d:c0:6b:86	Winstars Technology Ltd

Network Traffic Control: Enable - Defend - Protect

- Selecting the Check for Updates option from the right click context menu will check to see whether there are any newer versions of the Agent available. If there are, the user can choose to update the Agent.

Details

- After installation, when the user locks and unlocks the computer, or manually clicks on the icon in the system tray, the Drawbridge Agent will attempt to register the computer with the Drawbridge. If the registration is successful, the computer will be permanently linked to its associated local device in the console. This is a one time operation and will not be done again unless the user uninstalls and reinstalls the Agent.
- After the intial registration, or after any subsequent user logon, the Agent will then proceed to try to authenticate the current Windows user and link the Windows user to a console user. There will be a toast message displayed that shows the outcome of this authentication attempt.
- If for some reason a user is not able to register a computer with the Drawbridge, he should perform a Repair of the Agent by typing appwiz.cpl into the Windows start menu, then right clicking on the Drawbridge Agent item and selecting Uninstall/Change.


draw - Programs and Features
Control Panel › Programs › Programs and Features
draw
Control Panel Home
View installed updates
Turn Windows features on or off
Organize
Uninstall/Change
Uninstall/Change

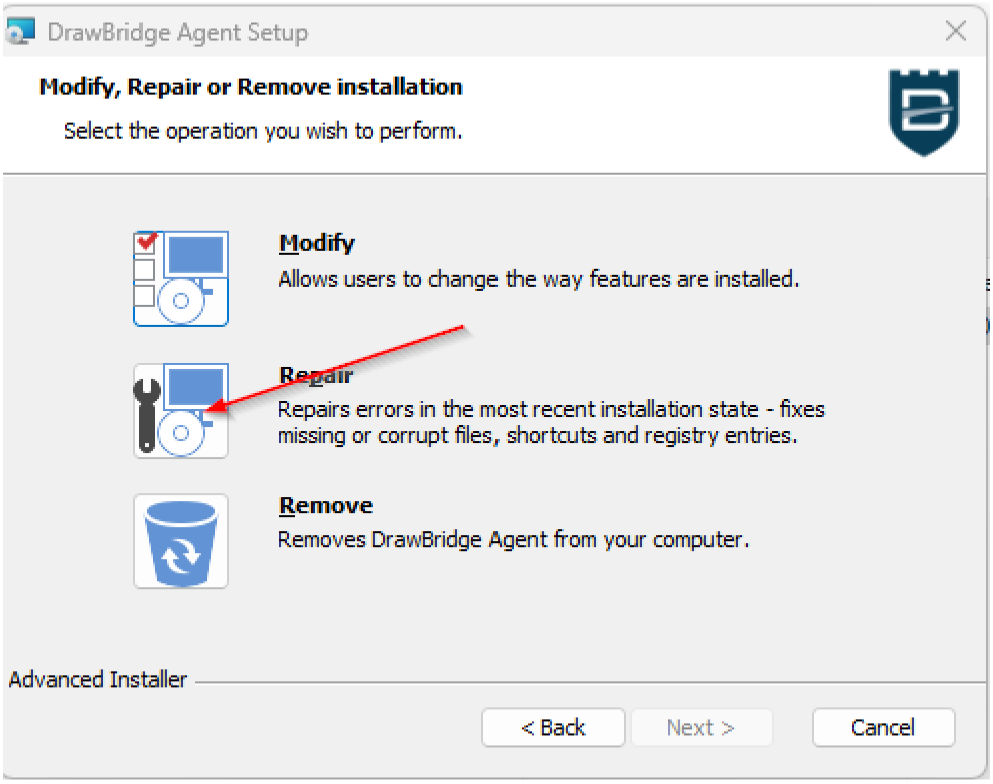
Uninstall or change a program

To uninstall a program, select it from the list and then click Uninstall, Change, or Repair.

Name	Publisher	Installed On	Size	Version
DrawBridge Agent	Compass Foundation	2022-09-28	99.3 MB	1.2.5

Compass Foundation Product version: 1.2.5 Support link: support@compassfou... Comments: This installer database contains the l...
Help link: support@compassfou... Size: 99.3 MB

This will then open another dialog where the user can confirm the repair.



Modify, Repair or Remove installation

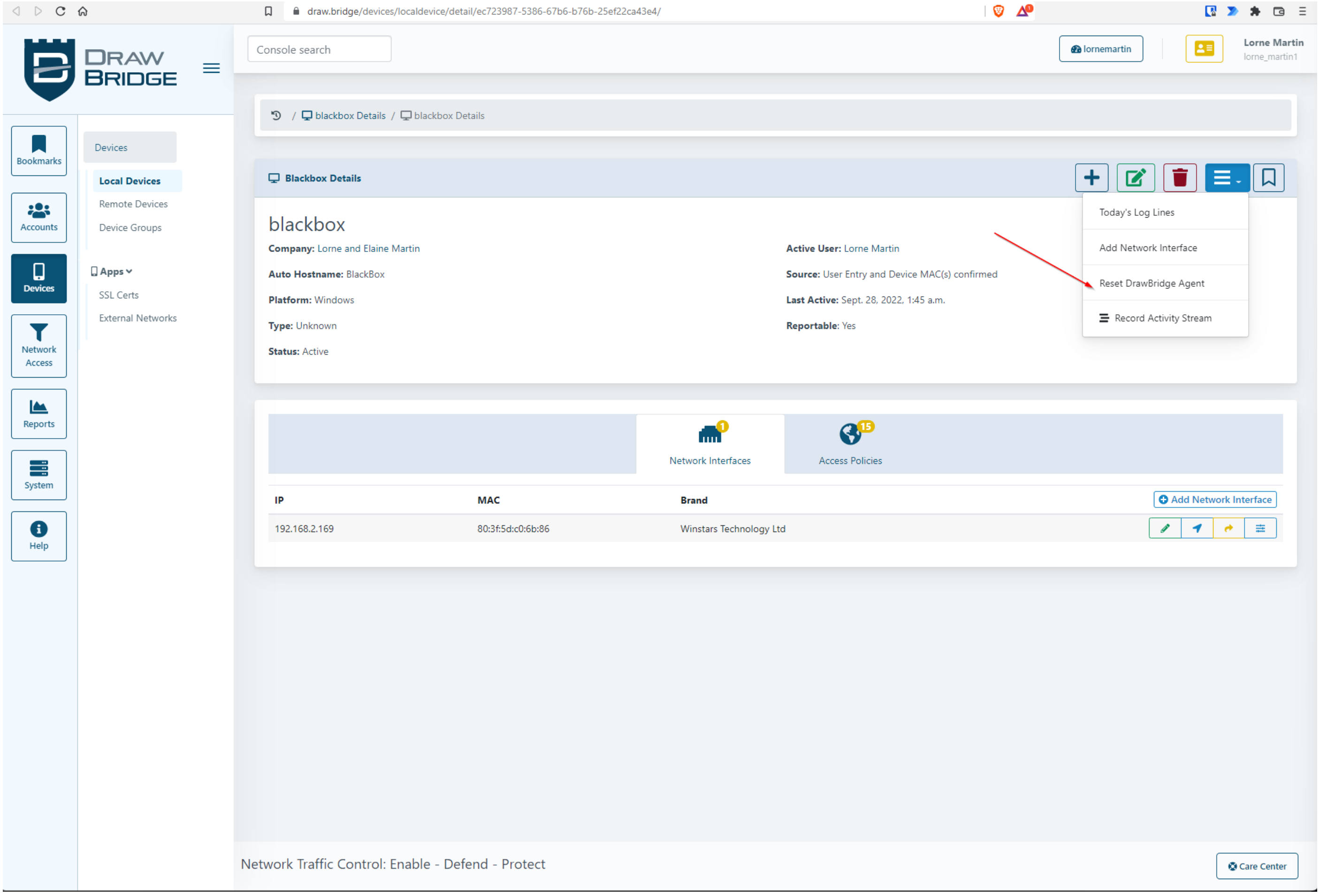
Select the operation you wish to perform.

Modify
Allows users to change the way features are installed.

Repair
Repairs errors in the most recent installation state - fixes missing or corrupt files, shortcuts and registry entries.

Remove
Removes DrawBridge Agent from your computer.

- When a user uninstalls the Agent, the Agent sends a request to the console to remove the association between the local device on the console, and the user's computer. If this for some reason fails, the user will not be able to succesfully reinstall and register the Agent with the console in the future. It is possible to manually reset this association by logging onto the console, and selecting the option to `Reset Drawbridge Agent` as shown below.



Blackbox Details

blackbox

Company: Lorne and Elaine Martin

Auto Hostname: BlackBox

Platform: Windows

Type: Unknown

Status: Active

Active User: Lorne Martin

Source: User Entry and Device MAC(s) confirmed

Last Active: Sept. 28, 2022, 1:45 a.m.

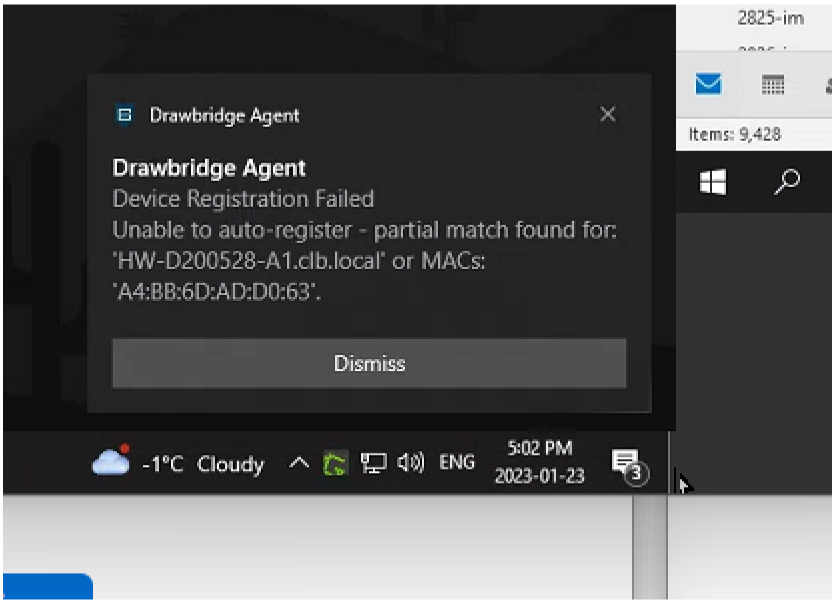
Reportable: Yes

IP	MAC	Brand
192.168.2.169	80:3f:5d:c0:6b:86	Winstars Technology Ltd

Network Traffic Control: Enable - Defend - Protect

Troubleshooting

Device Registration Failed - Unable to auto-register - partial match found



Drawbridge Agent

Device Registration Failed

Unable to auto-register - partial match found for: 'HW-D200528-A1.clb.local' or MACs: 'A4:BB:6D:AD:D0:63'.

In this case the local device on the console did not have the `clb.local` suffix so the Agent coudl not find a complete match. Upon further investigation, the local device record also had two interfaces defined, one with a MAC and IP, the other with only a MAC. Removing the interface with only the MAC address, and reinitializing the registration process fixed the problem. In summary, there will be an attempt made to match host names that only partially match local device names, but there will need to be a different definitive match found.

Check Agent logs for more details

The Agent records a log file in the `C:\Program Files (x86)\Compass Foundation\DrawBridge Agent\` folder. The file name is `Drawbridge Agent.log`.

The DrawBridge Agent reports that device Registration failed

An important note:

- Randomized MAC addresses are not supported for the auto-creation of Local Device records in the DrawBridge. If you have an endpoint that is using a randomized MAC address, either turn off Randomized addresses, OR, if it's a Virtual Machine, for example, and that's not an option, manually create the Local Device record in the DrawBridge console and Make Sure the Hostname field matches the actual Device hostname exactly. Then, when the DrawBridge Agent does the "tap" authentication operation, it will match up with the Local Device record based on the hostname.

Resolution: Search the Local Device list Interface column for the IP address of the device that's failing to register. Take note of the `Auto-Hostname` field and compare it to the actual Device hostname. These two must match for the registration to be successful.

The DrawBridge Agent local device Registration fails after domain-joining the device

If the DrawBridge Agent is deployed on a Local Device that is then joined to an AD domain at some future point, the Canonical ID for that Local Device record will then be in conflict because of the ID pulled from the Active Directory database.

Resolution: Delete the existing Local Device record; the correct Local Device record should be automatically generated at next sync.

Miscellaneous Tech Notes regarding AD Sync:

- AD Sync happens automatically 4 times a day, and can also be manually triggered.
- Both plain-text sync and encrypted sync are available. Encryption is strongly recommended: use port 636 to default to LDAPS.

Usage Example

- Tommy is a user in an AD database. He's assigned to the Warehouse AD Directory Group.
- The Drawbridge has synced over both Tommy the person as well as the Warehouse AD Directory Group, AND Tommy's membership in the Warehouse AD Directory Group.
- An Access Policy assigned to the Warehouse Device Group (of which the Warehouse AD Directory Group is a Proxy Users Group member) only allows access to Shipping and related business categories.
- Then Tommy gets promoted as a manager to the Strategic Warehouse Development & Improvements Team. The network admin adds Tommy to the Managers AD Directory Group.
- The DrawBridge also knows about the Managers AD Directory group group, and a policy already configured for that group allows access to additional categories for research purposes.
- When the network admin adds Tommy to the Managers AD Directory group, the DrawBridge synchronizes that information over, and Tommy automatically gets the increased content filter access without anyone needing to touch filter settings in the DrawBridge.