Maintenance Guide

ON THIS PAGE

Maintenance Guide

This guide describes how to perform recurring administrative operations in ForgeRock Access Management Web Agent.

About ForgeRock Identity Platform™ Software

ForgeRock® Identity Platform serves as the basis for our simple and comprehensive Identity and Access Management solution. We help our customers deepen their relationships with their customers, and improve the productivity and connectivity of their employees and partners. For more information about ForgeRock and about the platform, see https://www.forgerock.com.

Audit Web Agent

Web Agent logs audit events for security, troubleshooting, and regulatory compliance. Store agent audit event logs in the following ways:

Remotely
: Log audit events to the audit event handler configured in the AM realm. In an environment with several AM servers, agents write audit logs to the AM server that satisfies the agent request for client authentication or resource authorization.

  Web Agent cannot log audit events remotely if:

  - AM's Audit Logging Service is disabled.
  - No audit event handler is configured in the realm where the agent is configured.

- All audit event handlers configured in the realm where the agent is configured are disabled.

For more information about audit logging in AM, see Setting Up Audit Logging in AM's *Security Guide*.

Locally

Log audit events in JSON format to `/web_agents/agent_type/instances/agent_nnn/logs/debug/audit.log`. The following is an example agent log file: `/web_agents/nginx22_agent/instances/agent_1/logs/audit/audit.log`.

Remotely and locally

Log audit events:

- To `/web_agents/agent_type/instances/agent_nnn/logs/debug/audit.log`
- To the audit event handler configured in the AM realm in which the agent profile is configured.

The following is an example agent log record:


```
{
   "timestamp":"2017-10-30T11:56:57Z",
   "eventName":"AM-ACCESS-OUTCOME",
   "transactionId":"608831c4-7351-4277-8a5f-b1a83fe2277e",
   "userId":"id=demo,ou=user,dc=openam,dc=forgerock,dc=org",
   "trackingIds":[
      "fd5c8ccf-7d97-49ba-a775-76c3c06eb933-82095",
      "fd5c8ccf-7d97-49ba-a775-76c3c06eb933-82177"
   ],
   "component":"Web Policy Agent",
   "realm":"/",
   "server":{
      "ip":"127.0.0.1",
      "port":8020
   },
   "request":{
      "protocol":"HTTP/1.1",
      "operation":"GET"
   },
   "http":{
      "request":{
         "secure":false,
         "method":"GET",
         "path":"http://my.example.com:8020/examples/",
         "cookies":{
```

```
            "am-auth-jwt":"eyJ0eXAiOiJKV1QiLCJhbGciOi[...]"
            "i18next":"en",
            "amlbcookie":"01",
            "iPlanetDirectoryPro":"Ts2zDkGUqgtkoxR[...]"
         }
      }
   },
   "response":{
      "status":"DENIED"
   },
   "_id":"fd5c8ccf-7d97-49ba-a775-76c3c06eb933-81703"
}
```


NOTE

Local audit logs do not have an `_id` attribute, which is an internal AM id.

The audit log format adheres to the log structure shared across the ForgeRock Identity Platform. For more information about the audit log format, see Audit Log Format in AM's *Security Guide*.

Web Agent supports propagation of the transaction ID across the ForgeRock platform, using the HTTP header `X-ForgeRock-TransactionId`. For more information about configuring the header, see Configuring the Trust Transaction Header System Property in AM's *Security Guide*.

By default, Web Agent does not write audit log records. To configure audit logging, perform the following procedure:

Configure Audit Logging

By default, Web Agent does not write audit log records. To configure audit logging, perform this procedure. The agent in this example is in remote configuration mode.

1. In `OpenSSOAgentBootstrap.properties`, set values for the following properties:
   - Local Agent Audit File Name
   - Local Audit Log Rotation Size

     NOTE

     After changing a bootstrap property, restart the web server where the agent runs.

2. On the AM console, select REALMS > Realm Name > Applications > Agents > Web > Agent Name.
3. On the **Global** tab, select the following options to configure audit:
    - Agent Debug Level
    - Audit Access Types
    - Audit Log Location

Notifications

AM sends the following notifications to Web Agent through WebSockets:

Configuration notifications
When the administrator makes a change to a hot-swappable agent configuration property, AM sends a notification to the agent to reread the agent profile from AM.

Configuration notifications apply when the agent profile is stored in AM's configuration data store.

For more information about the cache, see Configuration Cache.

Session Notifications
When a client logs out, or a CTS-based session expires, AM sends a notification to the agent to remove the client's entry from the session cache.

For more information about the cache, see Session and Policy Decision Cache.

Policy Notifications
When an administrator changes a policy, AM sends a notification to the agent to flush the session and policy decision cache, and the policy cache.

For more information about the cache, see Session and Policy Decision Cache and Policy Cache.

In configurations with load balancers and reverse proxies, make sure that the load balancers and reverse proxies support WebSockets.

The AM advanced server configuration property, `org.forgerock.openam.notifications.agents.enabled`, controls whether the AM server sends notifications to connected agents. This property is enabled by default.

To Disable Notifications

CAUTION

CAUTION

Notifications are enabled by default. Before disabling notifications, consider the impact on security if the agent is not notified of changes in AM.

1. On the AM console, select REALMS > Realm Name > Applications > Agents > Web > Agent Name.
2. On the **Global** tab, deselect the following options to disable notifications:
   - Enable Notifications

     After changing this property, restart the web server where the agent runs.
   - Enable Notifications of Agent Configuration Change