SENTINELONE: CONFIGURE EXCLUSIONS

Security Validation validates the effectiveness of your security technologies. This is done by installing Actors in locations around your network. Endpoint security technologies running on the Actor may flag Mandiant services that are required to run Actions. In order for these Actors to be effective and carry out Actions, certain endpoint files pertaining to the execution of these Actors must be added to the allowlist with the security technologies installed on the host.

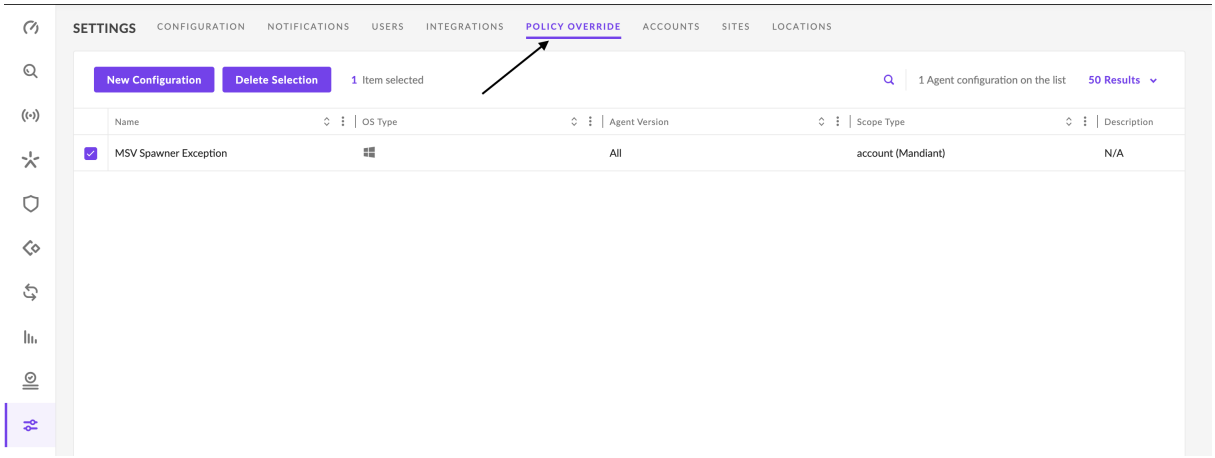
> The following information is based on the security technology manufacturer's documentation. If the steps do not match your UI, consult the technology's documentation directly.

When using Security Validation on a network that includes SentinelOne, the Mandiant Advantage team recommends configuring exclusions using the following process.

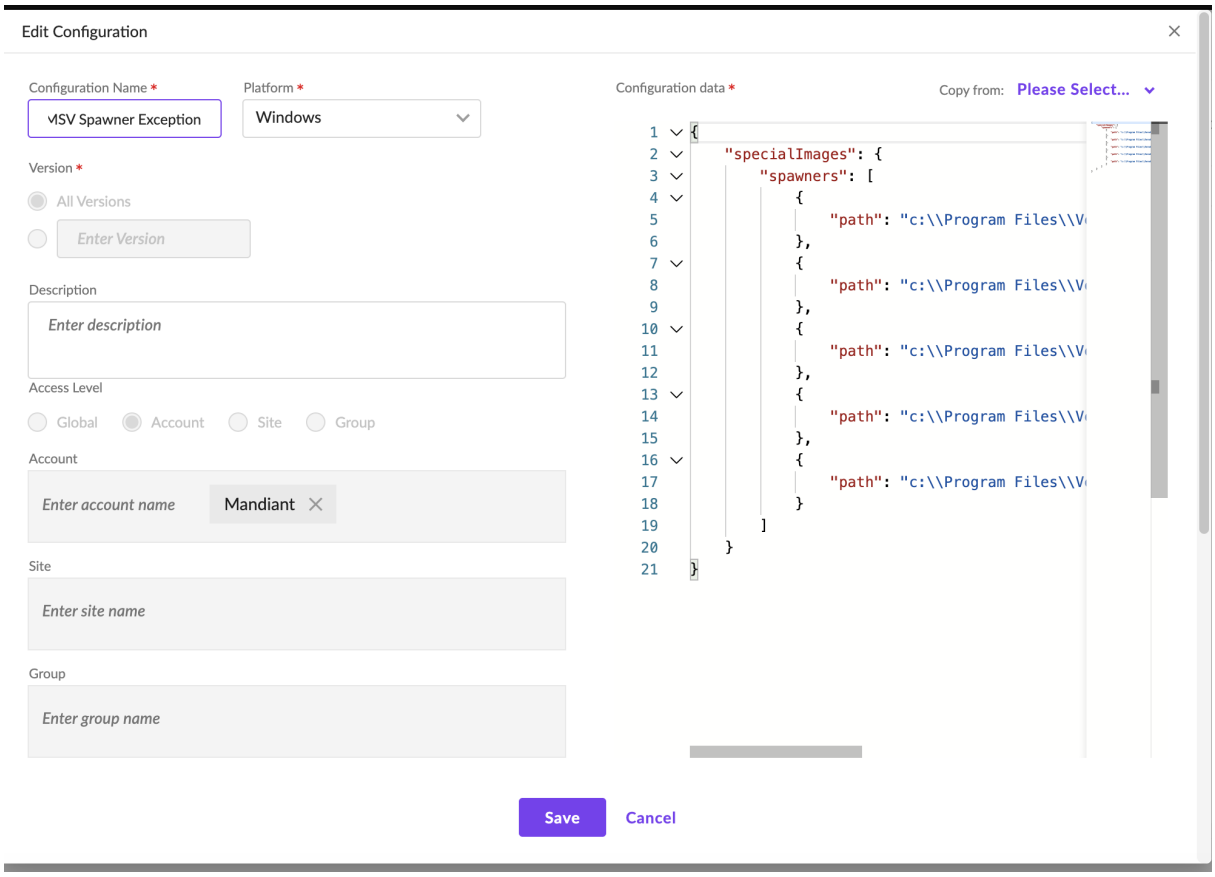
Configure Exclusions

The policy override for SentinelOne (S1) can be set up using the following steps.

1. Locate **SETTINGS** in the menu pane of the S1 management console.
2. Select **POLICY OVERRIDE** tab.



3. Select **New Configuration**.
4. Add a custom JSON policy override, which S1 calls a Spawner rule.
5. Enter **Name** and **Description** (optional).
6. Select either an Account, Site, or Group for this policy overrides to apply to.
7. Copy and paste the **JSON config** into the **Configuration data** pane.



8. **Save** the configuration.

JSON Exclusion Data

```
{
 "specialImages": {
   "spawners": [
     {
       "path": "c:\\Program Files\\Verodin\\node\\node\\scripts\\verodin_backend_service.exe"
     },
     {
       "path": "c:\\Program Files\\Verodin\\node\\node\\scripts\\verodin_backend.exe"
     },
     {
       "path": "c:\\Program Files\\Verodin\\node\\node\\scripts\\verodin_endpoint_service.exe"
     },
     {
       "path": "c:\\Program Files\\Verodin\\node\\node\\scripts\\cli_executer.exe"
     },
     {
       "path": "c:\\Program Files\\Verodin\\node\\node\\scripts\\change_user.exe"
     },
     {
       "path": "c:\\Program Files\\Verodin\\node\\node\\scripts\\verodin_network_service.exe"
     }
   ]
 }
}
```