



# Operational Intelligence

Deployment Guide

---

## User Guide

---

# Disclaimer

Honeywell International Inc. ("HII") reserves the right to make changes in specifications and other information contained in this document without prior notice, and the reader should in all cases consult HII to determine whether any such changes have been made. HII makes no representation or warranties regarding the information provided in this publication.

HII shall not be liable for technical or editorial errors or omissions contained herein; nor for incidental or consequential damages resulting from the furnishing, performance, or use of this material. HII disclaims all responsibility for the selection and use of software and/or hardware to achieve intended results.

This document contains proprietary information that is protected by copyright. All rights are reserved. No part of this document may be photocopied, reproduced, or translated into another language without the prior written consent of HII.

Copyright © 2026 Honeywell Group of Companies. All rights reserved.

Web Address: [automation.honeywell.com](https://automation.honeywell.com)

Elemex is a trademark of Biz2mobile Ltd.

Google, Android and other marks are trademarks of Google LLC.

Other product names or marks mentioned in this document may be trademarks or registered trademarks of other companies and are the property of their respective owners.

For patent information, refer to [www.hsmpats.com](https://www.hsmpats.com).

# TABLE OF CONTENTS

|                                                        |          |
|--------------------------------------------------------|----------|
| Customer Support .....                                 | v        |
| Technical Assistance .....                             | v        |
| <b>Chapter 1 - Overview .....</b>                      | <b>1</b> |
| Introduction .....                                     | 1        |
| Elemex Agent Deployment .....                          | 1        |
| <b>Chapter 2 - Network/IT Requirements.....</b>        | <b>3</b> |
| DNS .....                                              | 3        |
| Web Proxies Support.....                               | 3        |
| Server URLs/Addresses Used.....                        | 3        |
| Mobile Device Agent Requirements .....                 | 4        |
| Honeywell Cloud Connect (HCC) Requirements .....       | 4        |
| HCC Host PC Requirements.....                          | 4        |
| Web Dashboard Requirements.....                        | 5        |
| Application Whitelisting .....                         | 5        |
| Agnostic Packages .....                                | 6        |
| <b>Chapter 3 - Integrate BYOA and Deep Link .....</b>  | <b>7</b> |
| Definitions.....                                       | 7        |
| Requirements .....                                     | 7        |
| Bring Your Own Authentication (BYOA) Integration ..... | 8        |
| Bring Your Own Authentication Process Flow .....       | 9        |
| Deep Link Integration.....                             | 9        |

|                          |    |
|--------------------------|----|
| User Authorization ..... | 10 |
|--------------------------|----|

## **Chapter 4 - Android Agent Deployment ..... 11**

|                                                                      |    |
|----------------------------------------------------------------------|----|
| How the Elemez Android Agent Works .....                             | 11 |
| Deployment Options .....                                             | 12 |
| Elemez Agent Android Permissions.....                                | 13 |
| Elemez Extension Android Permissions .....                           | 14 |
| Enrolling a Device in Elemez.....                                    | 15 |
| Enterprise Firewall Requirements .....                               | 15 |
| UK Elemez Server.....                                                | 15 |
| The Elemez Enrollment Token .....                                    | 15 |
| General Enrollment Mechanism.....                                    | 16 |
| Manufacturer Specific Discussion .....                               | 16 |
| Zebra.....                                                           | 16 |
| Elemez Permissions on Zebra Devices.....                             | 17 |
| Samsung.....                                                         | 17 |
| Manual Deployments for Testing Purposes.....                         | 18 |
| Elemez Agent Only.....                                               | 18 |
| Elemez Agent and Extension.....                                      | 19 |
| Deployment via an EMM.....                                           | 20 |
| Use of Wildcards for Serial Number and IMEI.....                     | 20 |
| SOTI MobiControl .....                                               | 21 |
| Installation .....                                                   | 21 |
| Starting the Elemez Agent after deployment .....                     | 21 |
| Whitelisting Elemez for Power Management.....                        | 21 |
| Omnissa Workspace One UEM (Airwatch).....                            | 22 |
| Installation using the Legacy method .....                           | 22 |
| Ivanti Neurons for MDM (MobileIron) .....                            | 22 |
| Deployment using Android Enterprise from the Managed Play Store..... | 22 |
| Deployment using Android Enterprise from the Google Play Store.....  | 22 |
| Use of Wildcards .....                                               | 23 |
| Microsoft Intune.....                                                | 23 |
| 42Gears SureMDM .....                                                | 23 |
| Installation.....                                                    | 23 |

|                                                                       |           |
|-----------------------------------------------------------------------|-----------|
| Starting the Elemex Agent after deployment .....                      | 24        |
| Limitations .....                                                     | 24        |
| Scalefusion .....                                                     | 24        |
| Deployment using Android Enterprise from the Enterprise Store.....    | 24        |
| Starting the Elemex Agent after Deployment .....                      | 24        |
| Use of Wildcards .....                                                | 25        |
| Troubleshooting.....                                                  | 26        |
| <b>Chapter 5 - Zebra Agent Deployment .....</b>                       | <b>29</b> |
| Prerequisites .....                                                   | 29        |
| Deployment Method .....                                               | 29        |
| Configure the Elemex App .....                                        | 30        |
| Configure the Elemex Zebra Extension App .....                        | 31        |
| Configure the Zebra OEMConfig Profile .....                           | 31        |
| Zebra Android 10 Method.....                                          | 31        |
| Zebra Android 11 and 13 Method .....                                  | 32        |
| Zebra Android 14+ Method.....                                         | 32        |
| Enroll the Device.....                                                | 34        |
| <b>Chapter 6 - Samsung Agent Deployment.....</b>                      | <b>35</b> |
| Deployment Guide.....                                                 | 35        |
| Prerequisites.....                                                    | 35        |
| Deployment Method.....                                                | 35        |
| <b>Chapter 7 - Windows Agent Installation .....</b>                   | <b>39</b> |
| Check the Communications Path to the Elemex Cloud Platform .....      | 39        |
| Download the Elemex Agent for Windows .....                           | 39        |
| Install the Agent to Register the Device with the Cloud Service ..... | 40        |
| Uninstalling the Agent .....                                          | 40        |
| <b>Chapter 8 - Windows Agent Deployment with Intune.....</b>          | <b>41</b> |
| Deployment Guide .....                                                | 41        |
| Download the Required Utilities and Files .....                       | 42        |

|                                                                    |           |
|--------------------------------------------------------------------|-----------|
| Package the Elemez Token File for Deployment.....                  | 42        |
| Create PowerShell Scripts .....                                    | 42        |
| Package the Elemez Agent for Deployment .....                      | 43        |
| Add the Elemez Token File Package to Intune.....                   | 44        |
| Add the Elemez Agent Package to Intune .....                       | 44        |
| Deploy the Token File and Elemez Apps .....                        | 45        |
| Updating the Elemez Agent.....                                     | 45        |
| Upgrading the Agent to a Later Release .....                       | 45        |
| Downgrading the Agent to an Earlier Release.....                   | 45        |
| <b>Chapter 9 - Windows Agent Deployment with ScaleFusion .....</b> | <b>47</b> |
| Agent Deployment.....                                              | 47        |

# Customer Support

## Technical Assistance

To search our knowledge base for a solution or to log in to the Technical Support portal and report a problem, go to [www.automation.honeywell.com](http://www.automation.honeywell.com), and then select **Support > Productivity > Technical Support** to find a host of options to help you quickly find the support you need and/or who to contact.



## Introduction

This document describes requirements and methods for deploying Honeywell Operational Intelligence. Honeywell Operational Intelligence is a cloud-based insights and automation platform helping businesses optimize deployment and use of mobile technologies. It can provide proactive alerts, for example, to highlight potential problems such as battery degradation, frequent drops or excessive downtime. Then the software can trigger automated maintenance workflows to resolve issues without manual intervention.

Refer to the Operational Intelligence Device Support Matrix available at [automation.honeywell.com](https://automation.honeywell.com) for information on supported devices.

For more information about Honeywell Operational Intelligence, refer to the user guide available at [automation.honeywell.com](https://automation.honeywell.com).

## Elemesz Agent Deployment

The Honeywell Operational Intelligence platform utilizes the B2M Solutions Elemesz device agent and extension for collecting and reporting data from non-Honeywell devices. All references to Elemesz throughout this document are used in the context of supporting non-Honeywell devices within Honeywell's Operational Intelligence platform.

This is a generic guide and is meant to help signpost the configuration options you may need to make in support of deploying and auto-launching the Elemesz app in an Android Enterprise environment. The exact configuration method will depend on the Android Enterprise EMM platform that is in use.

Follow the instructions to deploy the Elemesz agent based on the type of device you are using.

- [Android Agent Deployment](#)
- [Zebra Agent Deployment](#)
- [Samsung Agent Deployment](#)

- [Windows Agent Installation](#)
- [Windows Agent Deployment with Intune](#)
- [Windows Agent Deployment with ScaleFusion](#)

# NETWORK/IT REQUIREMENTS

This chapter provides an overview of the network requirements to deploy Operational Intelligence.

## DNS

When Operational Intelligence is hosted on the cloud (internet), devices need to be able to resolve the cloud server hostnames via DNS. The list of server hostnames requiring DNS support is listed in the following section.

## Web Proxies Support

Devices connect to Operational Intelligence cloud servers via HTTPS and web sockets.

All connections can be proxied by HTTP/S web proxies and are outbound.

## Server URLs/Addresses Used

This section contains the list of server URLs and hostnames used by the Operational Intelligence services. These URLs need to be whitelisted in web proxies or firewall configurations to allow devices to connect to the cloud services.

**Note:** For Firewall proxies, it is recommended to whitelist FQDN instead of IP address. Even though Honeywell tries to keep the IP address list up to date, IP addresses might need to be added or modified to support scalability and availability of the solution. We try to add IP addresses observed from global locations, but we also recommend customers add additional IP addresses resolved for the following DNS based on their network topology.

# Mobile Device Agent Requirements

The device agent provides the core connectivity services for the devices to be able to connect to Operational Intelligence and send telemetry and event data.

**Note:** *To ensure an MDM client/policy does not stop Operational Intelligence from functioning, you must ensure that background/system applications are allowed to run and determine whether the Staging Hub Agent process (OI Agent) needs access privileges.*

| FQDN/DNS                                            | Port | Protocol |
|-----------------------------------------------------|------|----------|
| sentt02dprodv2.azure-devices.net                    | 443  | HTTP(S)  |
| remotecontrol.caidc.honeywell.com                   | 443  | HTTP(S)  |
| sps.api.honeywell.com                               | 443  | HTTP(S)  |
| caidc.apis.honeywell.com                            | 443  | HTTP(S)  |
| peerdiscovery.operationalintelligence.honeywell.com | 443  | HTTP(S)  |
| opintel-endpoints.honeywell.com                     | 443  | HTTP(S)  |
| storage.operationalintelligence.honeywell.com       | 443  | HTTP(S)  |
| opintel-storage-cdn-gwhhdecygdse3dn.a03.azurefd.net | 443  | HTTP(S)  |
| operationalintelligence.honeywell.com               | 443  | HTTP(S)  |
| authn.honeywell.com                                 | 443  | HTTP(S)  |

## Honeywell Cloud Connect (HCC) Requirements

Honeywell Cloud Connect (HCC) is software that acts as a gateway for the communication between printers and the cloud. HCC needs to be installed on a Windows machine operating in the same network as printers.

### HCC Host PC Requirements

- Windows Server 2022 16 CPU, 32GB RAM
- Browser: Google Chrome

| FQDN/DNS                                            | Port | Protocol |
|-----------------------------------------------------|------|----------|
| sentt02dprodv2.azure-devices.net                    | 443  | HTTP(S)  |
| caidc.apis.honeywell.com                            | 443  | HTTP(S)  |
| sps.api.honeywell.com                               | 443  | HTTP(S)  |
| storage.operationalintelligence.honeywell.com       | 443  | HTTP(S)  |
| opintel-endpoints.honeywell.com                     | 443  | HTTP(S)  |
| opintel-storage-cdn-gwhhdecygdse3dn.a03.azurefd.net | 443  | HTTP(S)  |
| operationalintelligence.honeywell.com               | 443  | HTTP(S)  |
| authn.honeywell.com                                 | 443  | HTTP(S)  |

# Web Dashboard Requirements

Users accessing the Operational Intelligence web dashboard will need access to the following endpoints.

| FQDN/DNS                                            | Port | Protocol |
|-----------------------------------------------------|------|----------|
| honeywell-privacy.my.onetrust.com                   | 443  | HTTP(S)  |
| *.honeywell.com                                     | 443  | HTTP(S)  |
| cdn.cookieclaw.org                                  | 443  | HTTP(S)  |
| geolocation.onetrust.com                            | 443  | HTTP(S)  |
| *.launchdarkly.com                                  | 443  | HTTP(S)  |
| *.openstreetmap.org                                 | 443  | HTTP(S)  |
| opintel-storage-cdn-gwhhdecygdse3dn.a03.azurefd.net | 443  | HTTP(S)  |
| unpkg.com                                           | 443  | HTTP(S)  |
| hon-opcenter.my.salesforce-sites.com                | 443  | HTTP(S)  |
| *.aptrinsic.com                                     | 443  | HTTP(S)  |

## Application Whitelisting

Whitelist the following application names to ensure seamless onboarding.

| Honeywell Application                         | Package Name                                       | Version                   |
|-----------------------------------------------|----------------------------------------------------|---------------------------|
| OpIntel Device Agent/SSClient/<br>StagingHub  | com.honeywell.tools.ssclient                       |                           |
| Check in/Check Out                            | com.honeywell.oi.cico                              |                           |
| Virtual Locker                                | com.honeywell.oi.virtuallocker                     |                           |
| FindMyDevice - BeaconDirection                | com.honeywell.beacondirection                      | 1.00.00.0329<br>and below |
| FindMyDevice - BeaconTransmitter              | com.honeywell.tools.beacontransmitter              | 1.00.00.0329<br>and below |
| FindMyDevice - BeaconTransmitter <sup>1</sup> | com.honeywell.tools.honeywellbeacon<br>transmitter | 1.00.00.0329<br>and above |
| FindMyDevice - BeaconDirection <sup>2</sup>   | com.honeywell.df.beacondirection                   | 1.00.00.0367<br>and above |
| FindMyDevice - BeaconTransmitter <sup>2</sup> | com.honeywell.df.beacontransmitter                 | 1.00.00.0367<br>and above |
| Edge Rules Engine                             | com.honeywell.tools.rulesengine                    |                           |
| Printer Management application                | com.honeywell.tools.btprinterapplication           |                           |
| Enterprise Provisioner                        | com.honeywell.tools.provisioner                    |                           |
| EZConfig                                      | com.honeywell.tools.ezconfig                       |                           |
| HonSetup                                      | com.honeywell.honsetup                             |                           |

| Honeywell Application | Package Name                                   | Version |
|-----------------------|------------------------------------------------|---------|
| Indoor Locationing    | com.honeywell.indoorpositioningscan<br>service |         |
| Smart Talk            | com.honeywell.smart_talk2                      |         |
| Smart Talk            | com.hon.smarttalk                              |         |

1. Private Play store
2. Play store compatible

## Agnostic Packages

Whitelist the following application names if you are using device agnostic Op Intel to collect information from non-Honeywell devices.

| Honeywell Application   | Package Name                                                                                                                                                       | Version |
|-------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------|
| Elemesz agent           | com.b2msolutions.elemesz                                                                                                                                           |         |
| Elemesz agent extension | com.b2msolutions.elemesz.extension.<br><i>manufacturer_name</i><br><br>Where <i>manufacturer_name</i> is the device<br>manufacturer (i.e., zebra, datalogic, etc.) |         |

# INTEGRATE BYOA AND DEEP LINK

This chapter provides information to assist ISVs (Independent Software Vendors), partners or other users interested in integrating a third party application into Operational Intelligence. This information is specifically aimed at configuring customer Identity Providers for deep linking from a third party application into Operational Intelligence.

## Definitions

- **BYOA** (Bring Your Own Authentication) - allows users to be authenticated to Operational Intelligence using a third party Identity Provider (IDP).

**Note:** *BYOA covers authentication only. User authorization requires the replication of users in Op Intel, which can be done manually through the UI or via API.*

- **Deep Link** - the ability to hyperlink into a specific function or feature within Operational Intelligence (e.g., Device Details Page).
- **OAuth2.0** is an industry standard framework that describes overarching patterns for granting authorization. The application using OAuth constructs a specific request for permissions to a third-party system - usually called an Identity Provider (IDP) - which handles the authentication process and returns an Access Token representing success.
  - <https://www.oauth.com/oauth2-servers/map-oauth-2-0-specs/>
- **OpenID Connect** is an OAuth extension which adds and strictly defines an ID Token for returning user information.
  - Refer to <https://openid.net/connect/> for more information.

## Requirements

- Op Intel bring your own authentication integration requires a third party IDP utilizing OAuth2.0 OpenID Connect flow.
- The configuration of Op Intel as an allowed application into a third Party IDP.

- Client ID, Client Secret, authorization URL, and token URL related to said integration.

## Bring Your Own Authentication (BYOA) Integration

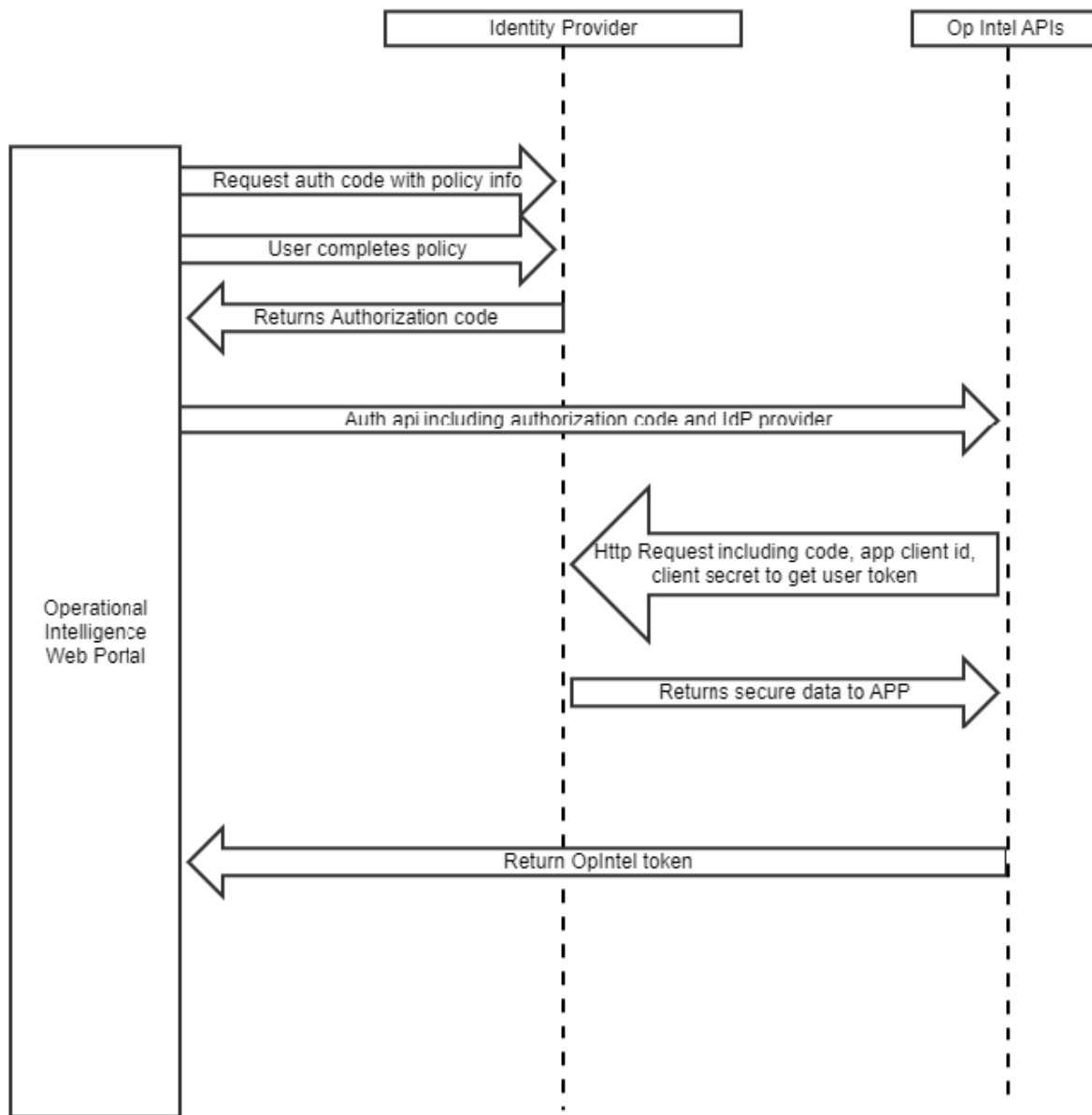
Op Intel Bring Your Own Authentication integration requires you to create an OAuth2.0 application in your IDP with the following parameters:

- Site: <https://operationalintelligence.honeywell.com/>
- Callback: <https://operationalintelligence.honeywell.com/oauth-callback>

The application creation process will return the following values that will need to be returned to Honeywell:

- **Client ID:** Identifies the Op Intel application in the third party IDP
- **Client Secret:** Shared secret used by Op Intel to authenticate a user
- **Authorization URL:** The third party IDP URL used by Op Intel to authenticate a user. Passed the Client ID and returned a one-time use authorization code.
- **Token URL:** The third party IDP URL used by Op Intel to request a JWT Token for the user. Passed the client ID, secret, and the one-time use authorization code (generated from the authorization URL).

# Bring Your Own Authentication Process Flow



## Deep Link Integration

Deep Link Integration relies on an authenticated user session. Any URL within Operational Intelligence can be hyperlinked to with an additionally passed query parameter (“authprovider”) which utilizes the associated IDP to identify the caller. An example would be a hyperlink to the device details page for a specific device:

<https://operationalintelligence.honeywell.com/assets/management/devices/CT4019021B3DDA?authprovider=customerdomain.com>

Where *CT4019021B3DDA* is the device serial number and *customerdomain.com* identifies the customer email domain. If *customerdomain.com* has BYOA integration in place, the above call would cause a redirection to the IDP configured for *customerdomain.com*. If the user already had an authenticated session with the customer IDP, a code would be returned to Operational Intelligence and the code would be exchanged for an ID token to get the user email to authorize within Operational Intelligence. If a valid user with this email existed in Operational Intelligence and was authorized to see the details of this device, the page would be rendered. If there was no authenticated user session after the redirection to the *customerdomain.com* IDP, the user would be presented the IDP user login page. Once logged in and authenticated, the user would be redirected to Op Intel, and the page would be rendered as previously described.

## User Authorization

BYOA covers user authentication but not authorization. Authorization is defined as what a user has access to in Operational Intelligence. To complete BYOA integration, a user account with a role must exist in Op Intel. This means that for every user in a third party system, a user with a matching email must exist in Op Intel. These users could be added manually through the OP Intel UI but more likely will be added by the third party system programmatically via API. Honeywell has user management APIs available in Op Intel for this purpose. Note that Operational Intelligence API access requires credentials (API key, Client ID and Secret) to successfully execute calls. Contact your Honeywell representative for more details.

# ANDROID AGENT DEPLOYMENT

This document describes best practices for deploying the Elemez Android agent and extension in both test and production environments.

**Note:** *For Panasonic Smart Essentials customers, the Smart Essentials service utilizes the B2M Elemez platform and Elemez Android agent. Note that the information in this document applies equally to Elemez and Smart Essentials versions of the product and service.*

## How the Elemez Android Agent Works

The Elemez agent is comprised of a main agent and an optional extension. In general, the main agent is used to extract Android metrics that are common to all device models and manufacturers. The extension is used for manufacturer-specific information retrieval as well as for information that might require elevated privileges from the device manufacturer.

The main agent is an application that is hosted on the Google Play store, or may otherwise be stored and deployed using the managed app store facility provided by an MDM/EMM platform. The agent is signed by B2M such that it cannot be updated by an application from any other source other than from B2M.

An extension may be signed by the device manufacturer. A manufacturer-signed extension provides the permissions necessary for Elemez to read privileged information such as the device identifiers (for Android 10+) and applications data usage and utilization information. Manufacturer-signed extensions must be deployed through a method other than from the Play store as Google does not allow B2M to host applications signed by a device manufacturer in B2M's Play store account. This is usually done by using the managed app store facility provided by most EMMs.

An extension may instead be provided directly by B2M, in which case it can be hosted on the Google Play store or may be stored and deployed using the managed app store facility provided by most EMMs. A B2M provided extension provides a subset of the information that is available from a manufacturer-signed extension. The types of metrics that will be available is dependent upon the manufacturer and model of the device and on the version of Android in use on that device.

In operation, the Elemez main agent will check for the presence of an extension and, if detected, will query the extension to retrieve the additional information that it provides. If there is no extension present, the main agent will retrieve as much information as it is able to with its own set of permissions.

The Elemez main agent Android package name is:

```
com.b2msolutions.elemez
```

The Elemez extension Android package name is:

```
com.b2msolutions.elemez.extension.manufacturer_name
```

where *manufacturer\_name* is “zebra”, “honeywell”, “datalogic”, etc.

The following extensions are available for the Elemez platform, providing the capabilities as listed in the table.

| Manufacturer | Type                | Capability                                                                                                                                                                                                                                                                            |
|--------------|---------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Datalogic    | Signed by Datalogic | Smart Battery Information<br>Application Metrics: Data Usage and Utilization Information<br>Device Identifiers: Serial Number, IMEI, SIM Serial Number                                                                                                                                |
| Honeywell    | Signed by Honeywell | Smart Battery Information<br>Application Metrics: Data Usage and Utilization Information<br>Device Identifiers: Serial Number, IMEI, SIM Serial Number                                                                                                                                |
| Panasonic    | Signed by Panasonic | Smart Battery Information<br>Application Metrics: Data Usage and Utilization Information<br>Device Identifiers: Serial Number, IMEI, SIM Serial Number                                                                                                                                |
| Zebra        | Provided by B2M     | Smart Battery Information<br>Application Metrics: Data Usage and Utilization Information (requires MX Framework 10.0+ on the device)<br>Device Identifiers Android 8, 9, 14: (Serial Number, IMEI, SIM Serial Number)<br>Device Identifiers Android 10, 11, 13: (Serial Number, IMEI) |

**Note:** *The list of extensions is expanding all the time. Check with your Honeywell representative if support for a manufacturer’s device not in the table above is required.*

## Deployment Options

The combinations of Elemez main agent, optional extension and deployment methods shown in the table below are possible and recommended.

In all cases where an agent and extension are to be deployed together, we strongly recommend that both applications are deployed from the same source, either from the Play store (if possible) or from the managed EMM store. Specifically, we do not recommend deploying the main agent from the Play store and the extension from

the managed EMM store as this may inadvertently cause invalid combinations of the main agent and extension versions if the Play store version is set to update automatically.

| Combination                                   | OS Version | Deployment Comments                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-----------------------------------------------|------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Main agent only                               | 8 - 9      | For all device types without an extension.<br>Can be deployed from the Play store using Managed Config to set the Token String for the target world. Use an intent or other means to launch the application after installation.<br>Can be deployed from the Play Store and started using an intent containing the Token String for the target world.<br>Can be deployed from an EMM managed app store and started using an intent containing the Token String for the target world.                                                                                                                                                                                                                                                                                        |
| Main agent only                               | 10+        | For all device types without an extension.<br>Can be deployed from the Play Store using Managed Config to set the Token String for the target world, the device Serial Number and, optionally, the device IMEI (for example, by using wildcards). Use an intent or other means to launch the application after installation.<br>Can be deployed from the Play Store and started using an intent containing the Token String for the target world, the device Serial Number and, optionally, the device IMEI (for example, by using wildcards).<br>Can be deployed from an EMM managed app store and started using an intent containing the Token String for the target world, the device Serial Number and, optionally, the device IMEI (for example, by using wildcards). |
| Main agent + manufacturer-signed extension    | 8 - 15     | For all device types with a manufacturer-signed extension. Should both be deployed from the EMM managed app store platform only and the main agent started using an intent containing the Token String for the target world.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Main agent + B2M provided extension for Zebra | 8 - 15     | For Zebra devices only.<br>Can be deployed from the Play Store using Managed Config to set the Token String for the target world. Use an intent or other means to launch the application after installation.<br>Can be deployed from the Play Store and the main agent started using an intent containing the Token String for the target world.<br>Can be deployed from an EMM managed app store and the main agent started using an intent containing the Token String for the target world.                                                                                                                                                                                                                                                                             |

## Elemz Agent Android Permissions

Elemz requires several normal and runtime Android permissions for the main agent.

| Permission Level | Permission                                                                                                                                                                                                                                                                                         |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| NORMAL           | ACCESS_NETWORK_STATE<br>ACCESS_WIFI_STATE<br>DOWNLOAD_WITHOUT_NOTIFICATION<br>FOREGROUND_SERVICE<br>INTERNET<br>QUERY_ALL_PACKAGES (A11+ only)<br>READ_NETWORK_USAGE_HISTORY<br>RECEIVE_BOOT_COMPLETED<br>REQUEST_COMPANION_RUN_IN_BACKGROUND<br>REQUEST_IGNORE_BATTERY_OPTIMIZATIONS<br>WAKE_LOCK |
| RUNTIME          | ACCESS_BACKGROUND_LOCATION (A10+ only)<br>ACCESS_COARSE_LOCATION<br>ACCESS_FINE_LOCATION<br>READ_EXTERNAL_STORAGE<br>READ_PHONE_STATE<br>WRITE_EXTERNAL_STORAGE                                                                                                                                    |

Normal level permissions require no special or explicit configuration. They are granted automatically by the Android OS.

Runtime level permissions must be explicitly granted for correct operation of the Elemez agent. This is generally achieved by granting each permission using adb for a manual installation or through use of the EMM for a centralized deployment.

## Elemez Extension Android Permissions

Signed Elemez extensions require several normal, runtime and signature level permissions.

| Permission Level | Permission                                                                |
|------------------|---------------------------------------------------------------------------|
| NORMAL           | QUERY_ALL_PACKAGES (A11+ only)<br>READ_NETWORK_USAGE_HISTORY<br>WAKE_LOCK |
| RUNTIME          | READ_EXTERNAL_STORAGE<br>READ_PHONE_STATE                                 |
| SIGNATURE        | BATTERY_STATS<br>PACKAGE_USAGE_STATS<br>READ_PRIVILEGED_PHONE_STATE       |

Normal level permissions require no special or explicit configuration. They are granted automatically by the Android OS.

Runtime level permissions must be explicitly granted for correct operation of the Elemez agent. This is generally achieved by granting each permission using adb for a manual installation or through use of the EMM for a centralized deployment.

Signature level permissions typically require signature level authorization from the device manufacturer through use of a manufacturer-signed extension. An extension that has been signed by the device manufacturer is granted signature level permissions automatically.

In some cases, the information retrieved using these permissions can alternatively be collected using a device manufacturer's SDK or manufacturer-specific APIs. The Elemex Zebra extension is such a case. The information required can generally be obtained from a Zebra device without requiring an extension signed by the manufacturer, Zebra.

## Enrolling a Device in Elemex

### Enterprise Firewall Requirements

To enable the device agent access from a firewalled enterprise location to the Elemex cloud server, the following configuration for the firewall is required. Note that the IP addresses may change over time, and although these are correct at the time of publication, we recommend performing a DNS lookup to resolve the IP addresses for the appropriate FQDN when required.

#### USA Elemex Server

- FQDNs: api.elemex.com, elemex.com, graph.elemex.com
- IP addresses: 54.83.18.223, 54.83.18.250
- Outbound port: TCP, 443

#### UK Elemex Server

- FQDNs: api.uk.elemex.com, uk.elemex.com, graph.uk.elemex.com
- IP addresses: 52.56.219.238, 18.130.19.143
- Outbound port: TCP, 443

## The Elemex Enrollment Token

The enrollment token is the piece of information that describes to the Elemex agent which Elemex data center and which Elemex world the device should enroll into.

If you have UI access to your Elemex world, then an admin level user can simply copy the token string from the enrollment menu option. The token string is then used either manually from an adb command prompt or via a script in the MDM/EMM to trigger enrollment of the agent into the correct world.

If you do not have UI access to your Elemenez world, then you can request the token string directly from B2M operations personnel. The token string can then be used in the same way as outlined above.

## General Enrollment Mechanism

A typical deployment for the agent and (optionally) the extension is:

1. Install the Elemenez main agent
  - a. Set the agent runtime permissions (via the EMM during install or manually after install).
  - b. Whitelist the agent for power management (via the EMM during install or manually after install).
2. Install the Elemenez extension (if required).
  - a. Set the extension runtime permissions (via the EMM during install or manually after install).
  - b. Whitelist the extension for power management (via the EMM during install or manually after install).
3. Start the Elemenez main agent using a script that provides the enrollment token to enroll the agent.

## Manufacturer Specific Discussion

### Zebra

In the past, the B2M Elemenez agent was included in the system image (ROM) shipped with various Zebra devices and on various versions of the Android OS. This was in support of a service offered by Zebra for which B2M provided the data collection. Therefore, deploying a new Elemenez instance on some Zebra devices may require an extra step to ensure that the Zebra OS does not interfere with the new Elemenez deployment on that device.

The following table describes how to mitigate for installing Elemenez on a device that has an existing version of Elemenez in the Zebra ROM, or for later versions of the Zebra OS that may otherwise interfere with the operation of the Elemenez agent. This behavior has been seen on the Zebra MC33 (Android 8.1).

| Android Version | Problem and Mitigation                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 8/9             | <p>When the Zebra OS detects an Elemez agent running on the device, it will stop that agent from operating unless one or both of these mitigations are deployed:</p> <p>Store a dummy file named ".001" in /sdcard. The OS will see this file and enable Elemez to operate normally.</p> <p>Disable the Zebra Data Analytics service by using the following XML code. This can be done by generating a bar code in Stage Now and scanning the bar code from the device, by deploying the commands directly from Stage Now, or by sending the commands to a device using a script from a suitable MDM/EMM platform.</p> <pre>&lt;wap-provisioningdoc&gt; &lt;characteristic version="4.2" type="AppMgr"&gt; &lt;parm name="Action" value="DisableApplication" /&gt; &lt;parm name="Package" value="com.symbol.dataanalytics" /&gt; &lt;/characteristic&gt; &lt;characteristic version="4.2" type="AppMgr"&gt; &lt;parm name="Action" value="DisableApplication" /&gt; &lt;parm name="Package" value="com.symbol.dataanalytics.dca" /&gt; &lt;/characteristic&gt; &lt;characteristic version="4.2" type="AppMgr"&gt; &lt;parm name="Action" value="DisableApplication" /&gt; &lt;parm name="Package" value="com.symbol.mxmfc.csp.analyticsmgr" /&gt; &lt;/characteristic&gt; &lt;/wap-provisioningdoc&gt;</pre> |
| 10              | <p>Several Zebra models running early versions of Android 10 firmware will also disable Elemez from operating. In this case, the remedy is to update the DA Agent on the device to the latest version to prevent this from happening.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| 11+             | <p>Zebra Android 11+ devices ship with a version of the DA Agent that ignores Elemez on the device and therefore no mitigation is required.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

## Elemez Permissions on Zebra Devices

The Elemez Android agent uses Zebra's MX Framework to set the PACKAGE\_USAGE\_STATS permission required by the agent to collect and report on application details on the device. This setting requires MX Framework version 10.0 or higher. Generally, this version of MX is found only on Zebra devices running Android 8.1 or higher.

Zebra normally provides the version of MX that is bundled with the firmware for a BSP or LifeGuard update in the appropriate Release Notes for that update.

If MX 10 or higher is available, then Elemez will report device data usage and application usage/data usage details.

If MX 10 or higher is not available in the device firmware, then device data usage and application usage/data usage details will not be reported, however all other parameters, metrics and events for the device will continue to be reported correctly.

## Samsung

There is no extension available for Samsung devices.

It is not possible to read the device Serial Number or IMEI on Samsung devices with Android OS 10+ and therefore the Serial Number and, optionally, the IMEI, MUST be provided to the Elemez agent from either the adb command line or from the MDM/EMM within a script or activity.

It is not possible to read the SIM Serial Number on Samsung devices.

Samsung devices generally have fixed, dumb (non-serialized, non-smart) batteries and therefore it is not possible to report on battery metrics such as manufacture date, serial number, health, capacity, etc.

For Samsung devices running Android 13 or higher, it is possible to use Samsung's Knox Service Plugin (KSP) to grant the Elemez agent the PACKAGE\_USAGE\_STATS permission for retrieving device data usage, application usage, application data usage metrics. Configure the following parameters in KSP to enable this permission and to whitelist the agent for power management.

## Manual Deployments for Testing Purposes

### Elemez Agent Only

In scenarios where the agent only is being deployed, use ADB to manually install the agent and grant the required permissions on a test device. This method requires a local connection between the PC running the command and the device and relies on knowledge of how to use the ADB tool.

Use the following method in the order in which the steps are described only.

1. Put the device into Developer Mode:  
Settings > About > Build Number > Click/Tap 5 times System > Developer Options and Enable USB Debugging

Connect the device to your PC using a USB cable and accept the authorization message that appears on the device.

2. Install the Elemez main agent. The -r flag causes any existing version of the APK on the device to be replaced. The -g flag grants all runtime permissions to the application. Substitute the correct filename as applicable.

```
adb install -r -g elemez.apk
```

3. Start the Elemez service (substitute the token string for the Elemez world for token\_string):

```
adb shell am start -n com.b2msolutions.elemez/.activities.AutoEnrolmentActivity -a com.b2msolutions.elemez.MDM_TOKEN_ACTION -e "token" "token_string"
```

Optionally, provide the serial number and IMEI for the device if required:

```
adb shell am start -n com.b2msolutions.elemez/.activities.AutoEnrolmentActivity -a com.b2msolutions.elemez.MDM_TOKEN_ACTION -e "token" "token_string" -e "serial" "serial_number_value" -e "imei" "imei_value"
```

#### 4. Whitelist the Elemez agent.

```
adb shell dumpsys deviceidle whitelist +com.b2msolutions.elemez
```

**Note:** The “adb install -g” method may additionally grant the `PACKAGE_USAGE_STATS` permission for the Elemez application on your test device. This will enable Elemez to report device data usage, application usage and application data usage metrics. This permission is not generally granted through an EMM/MDM, and therefore, results from the test environment may differ from results in a production environment when using Elemez without an OEM-specific extension.

## Elemez Agent and Extension

In scenarios where the agent and extension are being deployed, use ADB to manually install the agent and extension and to grant the required permissions on a test device. This method requires a local connection between the PC running the command and the device and relies on knowledge of how to use the ADB tool.

1. Put the device into Developer Mode:  
Settings > About > Build Number > Click/Tap 5 times System > Developer Options and Enable USB Debugging

Connect the device to your PC using a USB cable and accept the authorization message that appears on the device.

2. Install the Elemez extension. The -r flag causes any existing version of the APK on the device to be replaced, the -g flag grants all runtime permissions to the application. Substitute the correct filename as applicable.

```
adb install -r -g elemez-extension.apk
```

3. Install the Elemez main agent (substitute the correct filename as applicable).

```
adb install -r -g elemez.apk
```

Start the Elemez service (substitute the token string for the Elemez world for token\_string):

```
adb shell am start -n com.b2msolutions.elemez/.activities.AutoEnrolmentActivity -a com.b2msolutions.elemez.MDM_TOKEN_ACTION -e "token" "token_string"
```

Optionally, provide the serial number and IMEI for the device if required:

```
adb shell am start -n com.b2msolutions.elemez/.activities.AutoEnrolmentActivity -a com.b2msolutions.elemez.MDM_TOKEN_ACTION -e "token" "token_string" -e "serial" "serial_number_value" -e "imei" "imei_value"
```

4. Whitelist the Elemez main agent and extension (substitute the correct manufacturer package name as applicable)

```
adb shell dumpsys deviceidle whitelist +com.b2msolutions.elemez
adb shell dumpsys deviceidle whitelist
+com.b2msolutions.elemez.extension.manufacturer_name
```

**Note:** The “adb install -g” method may additionally grant the `PACKAGE_USAGE_STATS` permission for the Elemez application on your test device. This will enable Elemez to report device data usage, application usage and application data usage metrics. This permission is not generally granted through an EMM/MDM, and therefore, results from the test environment may differ from results in a production environment when using Elemez without an OEM-specific extension.

## Deployment via an EMM

This section discusses the general method for deploying the agent to devices remotely using an EMM platform.

### Use of Wildcards for Serial Number and IMEI

Under some conditions, it is not possible for the Elemez agent to read the serial number or IMEI directly from the device. This is generally when the device is running Android 10+ and there is no extension available.

In this case, the EMM must provide this information directly to the agent on deployment. This can be achieved in two ways:

1. By providing the serial number and IMEI within the same intent used to start and enroll the main agent.
2. By providing the serial number and IMEI using the Android Enterprise Managed Config method, where available.

Both of these methods rely on the capability of the EMM to substitute the actual value of the serial number and IMEI for a wildcard string at the time of the deployment. For example, some MDM/EMM platforms might use the string `$serialnumber$` in a script or in a Managed Config template and then substitute the actual value of the serial number for the device during deployment.

# SOTI MobiControl

## Installation

Deploy the agent and extension (if required) to the device using normal deployment procedures. Ideally, put the agent and extension into the same package. Ensure that the option to “Automatically Execute” the agent or extension when adding the APK to the package is unchecked (not selected). Ensure the applications are whitelisted for power management and that all required runtime permissions have been granted.

## Starting the Elemez Agent after deployment

To start the agent once deployed, we recommend using the following script from within MobiControl.

```
sleep 30
sendintent -a
"intent:#Intent;action=com.b2msolutions.elemez.MDM_TOKEN_ACTION;
component=com.b2msolutions.elemez/
.activities.AutoEnrolmentActivity;S.token=***;end"
sleep 30
```

Where “\*\*\*” is replaced by the token string in the script.

To start the agent and to provide the value for the device Serial Number and (optionally) IMEI once the agent is deployed, we recommend using the following script from within MobiControl:

```
sleep 30
sendintent -a
"intent:#Intent;action=com.b2msolutions.elemez.MDM_TOKEN_ACTION;
component=com.b2msolutions.elemez/
.activities.AutoEnrolmentActivity;S.token=***;S.serial=%SERIALNUM%
M%;S.imei=%IMEI%;end"
sleep 30
```

As the script is sent to each device, MobiControl will replace the %SERIALNUM% and %IMEI% wildcard values with the actual values for that device. This is required only for those cases where the Elemez agent is unable to read these values directly.

## Whitelisting Elemez for Power Management

To whitelist the Elemez agent and extension, SOTI provides a post-install script option.

For example, to whitelist Elemez on a Honeywell device, the following commands would be used:

```
batteryoptimize disable com.b2msolutions.elemez
batteryoptimize disable
com.b2msolutions.elemez.extension.honeywell
```

On Honeywell devices enrolled as Android Enterprise Work Managed, a minimum version of the MobiControl agent version 15.0.1 is required. On Honeywell devices enrolled as Android Classic, a minimum MobiControl agent version 15.1.0 is required. For further information visit <https://discussions.soti.net/articles/exempt-apps-from-doze-mode-on-honeywell-work-managed-devices>.

## Omnissa Workspace One UEM (Airwatch)

### Installation using the Legacy method

Create a product that first installs the extension (if required), and then the Elemez Android agent.

Create another product that runs a file/action containing a Run Intent with the following content:

```
mode=explicit,broadcast=false,action=com.b2msolutions.elemez.MDM_TOKEN_ACTION,package=com.b2msolutions.elemez,class=com.b2msolutions.elemez.activities.AutoEnrolmentActivity,extraString=token=<token>
```

...where <token> is replaced by your token string.

Set a dependency so that the second product runs only after the first product has finished installing the APKs.

Ensure the agent is whitelisted for power management and that all required runtime permissions have been granted.

## Ivanti Neurons for MDM (MobileIron)

### Deployment using Android Enterprise from the Managed Play Store

Add the Elemez agent and extension to the Managed Play Store. Deploy the agent and extension (if required) to the device using normal deployment procedures. Ensure the applications are whitelisted for power management and that all required runtime permissions have been granted.

### Deployment using Android Enterprise from the Google Play Store

If deploying the agent and extension (or agent only) from the Play Store, it is possible to use Managed Configuration to set parameters for the agent, including the token string.

If the agent/extension is able to read the device identifiers on the device (e.g., serial number and IMEI), then complete the token string field in the Elemez managed configuration settings and select “Auto-launch on install” to start the Elemez agent.

**Elemez**  
For Android Enterprise (Android for Work)

**Managed Configurations**  
Apply these configurations to the app when silently distributed to the users.

- ☐ Blocks app from sharing widget across profiles.
- ☐ Blocks the user from uninstalling the app.
- ☐ Minimum version code
- ☐ Auto-launch on install

Managed Configurations ?

| Configuration Name | Value                |
|--------------------|----------------------|
| Token              | <input type="text"/> |
| Serial Number      | <input type="text"/> |
| IMEI               | <input type="text"/> |

## Use of Wildcards

If the agent/extension is not able to read the device identifiers on the device (e.g., serial number and IMEI), then complete the token string field in addition to the Serial Number and IMEI fields in the managed configuration and select “Auto-launch on install” to start the Elemez agent.

MobileIron allows the use of wildcards in these fields. To auto-populate these fields for the target device from the MobileIron database, use the values “\${deviceSN}” for the Serial Number field and “\${deviceIMEI}” for the IMEI field.

## Microsoft Intune

Microsoft’s Intune UEM is a special case of an Android Enterprise EMM deployment for Elemez. Details for the use of Intune with Elemez can be provided in a separate document upon request.

## 42Gears SureMDM

### Installation

Either sideload the agent and extension into the SureMDM Managed Play Store or select the agent and extension from the Google Play store and add to the SureMDM Managed Play Store. Deploy the agent and extension to the device using normal procedures. Ensure the applications are whitelisted for power management and that all required runtime permissions have been granted.

## Starting the Elemez Agent after deployment

Configure and deploy a job ("Run Script") in SureMDM with the following content:

```
am start -n com.b2msolutions.elemez/.activities.AutoEnrolmentActivity -a com.b2msolutions.elemez.MDM_TOKEN_ACTION -e "token" "****"
```

Where "\*\*\*\*" is replaced by the token string for the world.

## Limitations

To deploy Elemez for agent-only profiles on Android 10 and higher, use the Android Enterprise Google Play store option, then use Managed Config for the Elemez application to set the Serial Number field to the wildcard "\$serialnumber\$". This will send the serial number to the agent and then the script will start the agent using that serial number .

Managed configuration

Configuration name  
Test

4 / 100

Token

Configure

Serial Number

✓ Configured

\$serialnumber\$

14 / 5000

It is not possible with SureMDM to treat the IMEI value in the same way.

## Scalefusion

### Deployment using Android Enterprise from the Enterprise Store

Add the Elemez agent and extension (if required) to the Scalefusion Enterprise Store. Ensure the applications are whitelisted for power management and that all required runtime permissions have been granted. Deploy the agent and extension as normal.

## Starting the Elemez Agent after Deployment

Create a Launch Activity and apply the activity to the device or devices.

- Mode: Explicit
- Action: com.b2msolutions.elemez.MDM\_TOKEN\_ACTION

- Package: com.b2msolutions.elemez
- Class Name: com.b2msolutions.elemez.activities.AutoEnrolmentActivity
- Extras 1:
  - Type: String
  - Key: token
  - Value: \*\*\*

Where “\*\*\*” is replaced by the token string for the world.

## Use of Wildcards

If the agent/extension is not able to read the device identifiers on the device (e.g., serial number and IMEI), then complete the token string field in addition to extras for the Serial Number and IMEI fields.

Scalefusion allows the use of wildcards in these fields. To auto-populate these fields for the target device from the Scalefusion EMM, use the values “\$device.serial\_no ” for the Serial Number field and “\$device.imei\_no ” for the IMEI field.

- Mode: Explicit
- Action: com.b2msolutions.elemez.MDM\_TOKEN\_ACTION
- Package: com.b2msolutions.elemez
- Class Name: com.b2msolutions.elemez.activities.AutoEnrolmentActivity
- Extras 1:
  - Type: String
  - Key: token
  - Value: \*\*\*
- Extras 2:
  - Type: String
  - Key: serial
  - Value: \$device.serial\_no
- Extras 3:
  - Type: String
  - Key: imei
  - Value: \$device.imei\_no

Where “\*\*\*” is replaced by the token string for the world.

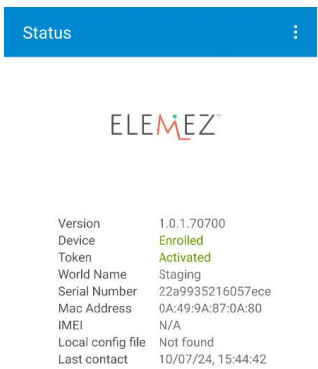
# Troubleshooting

The most likely problem to arise when installing and running the agent is that the device will fail to register with the server. There are several potential reasons for this:

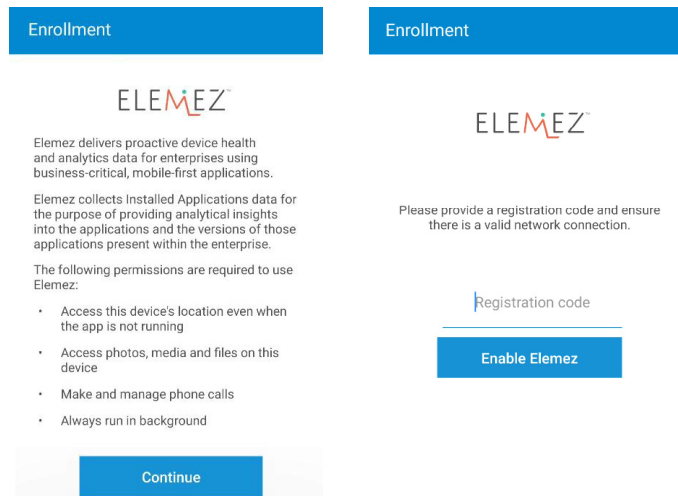
- The IP path to the server is blocked, typically by a firewall.
- The script for starting the agent by sending an intent has been entered incorrectly. Common mistakes are to add line breaks in those cases where you must enter the intent as a single long string or to copy and paste from another source and accidentally incorporate control characters into the string.
- The token string has been entered incorrectly and the agent cannot decrypt and use its contents to determine the correct data center or customer world to register the device with.
- The agent cannot determine the serial number to use for registration, either because it cannot read it from the device directly or it has not been provided to the agent using the managed config method, or within the script that starts the agent after installation.

Registration failure can generally be identified by starting the Elemez UI on the device.

If the UI presents a button for “STATUS” and clicking through shows that the device is enrolled, the token is activated and the world name is present, then the device has registered correctly and you should see it appear in the Elemez UI.



If the UI presents screens such as that below then the agent is not registered.



Check that:

- The device can open a browser session to [uk.elemez.com](https://uk.elemez.com) or [elemez.com](https://elemez.com) (for the UK and USA data centers respectively).
- The script command is correctly formatted and has been sent to the device and agent.
- The script contains the correct value for the Elemez token.
- The serial number of the device has been made available to the agent, either implicitly through using an extension or explicitly through providing the serial number in managed config, or by providing the serial number in the script that starts the agent.



# ZEBRA AGENT DEPLOYMENT

This chapter describes best practices for deploying the Elemex Android device agent to Zebra devices using a generic Android Enterprise model. It assumes familiarity with Android Enterprise, Managed Config, and OEMConfig methods.

## Prerequisites

There are several methods for deployment. The method to use depends on the versions of Zebra's MX framework and Android OS on the target devices. This table describes the options:

| Android OS | MX Version     | Method                                                             |
|------------|----------------|--------------------------------------------------------------------|
| 10         | 10.0 or higher | Use Zebra Legacy OEMConfig app and XML launch method.              |
| 11         | 10.0 or higher | Use Zebra OEMConfig Powered by MX app and XML launch method.       |
| 13         | 10.0 or higher | Use Zebra OEMConfig Powered by MX app and XML launch method.       |
| 14+        | 14.0 or higher | Use Zebra OEMConfig Powered by MX app and OEMConfig launch method. |

## Deployment Method

The general steps for deploying Elemex to Zebra devices using an Android Enterprise platform are:

1. Add the Elemex app from the Google Play™ store to the EMM.
2. Add the Elemex Zebra Extension app from the Google Play store to the EMM.
3. Add “Legacy Zebra OEMConfig” or “Zebra OEMConfig Powered by MX” from the Google Play store to the EMM.
4. Configure the Elemex app Managed Config information. See [Configure the Elemex App](#) on page 30.

5. Configure the Zebra OEMConfig profile to auto-launch the Elemesz app after installation. Note that there are different methods based on the Android version in use. See [Zebra Android 10 Method](#) on page 31, [Zebra Android 11 and 13 Method](#) on page 32, or [Zebra Android 14+ Method](#) on page 32.
6. Send the apps and OEMConfig profile to the device. The app will auto-launch and register with the Elemesz platform. See [Enroll the Device](#) on page 34.

## Configure the Elemesz App

Create a profile for the Elemesz App in the EMM. The app configuration profile must be set up as described below.

- You must grant the required runtime permissions for Elemesz. You may be able to choose to auto-grant all permissions to the app or to grant each requested permission independently, dependent upon the EMM platform in use.
- In the Managed Config settings for the Elemesz app, add a “Token” key (mandatory). The Token will be provided to you by your Honeywell representative.

The example below shows how these settings may be configured using Microsoft's Intune UEM.

[Home](#) > [Apps | Configuration](#) > [Elemesz Managed Config](#)

### Elemesz Managed Config | Properties ...

◇ <<

① Overview

▼ Manage

 Properties

> Monitor

#### Basics [Edit](#)

|                        |                        |
|------------------------|------------------------|
| Name                   | Elemesz Managed Config |
| Description            | No Description         |
| Device enrollment type | Managed devices        |
| Platform               | Android Enterprise     |
| Profile Type           | All Profile Types      |
| Targeted app           | Elemesz                |

#### Settings [Edit](#)

##### Permissions

| Permission                   | Permission state | Permission name            | Permission group |
|------------------------------|------------------|----------------------------|------------------|
| External storage (write)     | Auto grant       | WRITE_EXTERNAL_STORAGE     | STORAGE          |
| External storage (read)      | Auto grant       | READ_EXTERNAL_STORAGE      | STORAGE          |
| Phone state (read)           | Auto grant       | READ_PHONE_STATE           | PHONE            |
| Location access (background) | Auto grant       | ACCESS_BACKGROUND_LOCATION | LOCATION         |
| Location access (coarse)     | Auto grant       | ACCESS_COARSE_LOCATION     | LOCATION         |
| Location access (fine)       | Auto grant       | ACCESS_FINE_LOCATION       | LOCATION         |

##### Configuration Settings

| Configuration key | Value type | Configuration value                 |
|-------------------|------------|-------------------------------------|
| Token             | string     | AqrFJDclJwhrjaaDeKmX/WapkDM8VmnMGLj |

Connected apps

Not configured

# Configure the Elemez Zebra Extension App

The configuration profile should grant the required runtime permissions for the Elemez Zebra extension. The example below shows how these settings may be configured using Microsoft's Intune UEM.

[Home](#) > [Apps](#) | [Configuration](#) > [Zebra Elemez Extension](#)

## Zebra Elemez Extension | Properties

Search

Overview

Manage

Properties

Monitor

Name

Description

Device enrollment type

Platform

Profile Type

Targeted app

Zebra Elemez Extension

No Description

Managed devices

Android Enterprise

All Profile Types

Elemez Zebra Extension

Settings

Edit

Permissions

| Permission              | Permission state | Permission name       | Permission group |
|-------------------------|------------------|-----------------------|------------------|
| Phone state (read)      | Auto grant       | READ_PHONE_STATE      | PHONE            |
| External storage (read) | Auto grant       | READ_EXTERNAL_STORAGE | STORAGE          |

# Configure the Zebra OEMConfig Profile

There are several different methods for this, dependent upon which version of the Android OS is in use on the target device. Each method is outlined here.

## Zebra Android 10 Method

Use the Legacy Zebra OEMConfig app to add a new transaction step.

Under Device Administration Configuration, select the action as “Submit XML” and copy the following XML code into the “Submit XML” text box:

```
<wap-provisioningdoc>
  <characteristic version="9.2" type="Intent">
    <parm name="Action" value="StartActivity"/>
    <parm name="ActionName" value="android.intent.action.MAIN"/>
    <parm name="Type" value="explicit"/>
    <parm name="Package" value="com.b2msolutions.elemez"/>
    <parm name="Class"
value="com.b2msolutions.elemez.activities.AutoEnrolmentActivity"
/>
  </characteristic>
</wap-provisioningdoc>
```

This code will auto-launch the Elemez app after installation.

The example below shows this configuration using 42Gears SureMDM platform:

Save the OEMConfig configuration.

## Zebra Android 11 and 13 Method

Use the Zebra OEMConfig Powered by MX app.

Under System Configuration, copy the following XML code into the Pass-Through Command text box:

```
<wap-provisioningdoc>
  <characteristic version="9.2" type="Intent">
    <parm name="Action" value="StartActivity"/>
    <parm name="ActionName" value="android.intent.action.MAIN"/>
    <parm name="Type" value="explicit"/>
    <parm name="Package" value="com.b2msolutions.elemez"/>
    <parm name="Class"
value="com.b2msolutions.elemez.activities.AutoEnrolmentActivity"
/>
  </characteristic>
</wap-provisioningdoc>
```

This code will auto-launch the Elemez app after installation.

The example below shows this configuration using 42Gears SureMDM platform.

Save the OEMConfig configuration.

## Zebra Android 14+ Method

Use the Zebra OEMConfig Powered by MX app.

Follow these steps to configure the OEMConfig fields correctly:

1. Add a Package Configuration.
2. Within the Package Configuration, configure these fields:

- Class name: com.b2msolutions.elemez.activities.AutoEnrolmentActivity
- Package name: com.b2msolutions.elemez
- Package Signing Certificate: (see below)

3. Add a Feature Variance to the package.

4. Select the Feature Variance type as “Launch App after install/upgrade”.

The Package Signing Certificate is as follows:

```
MIIDcDCCAligAwIBAgIET2ikiTANBgkqhkiG9w0BAQUFADB6MQswCQYDVQQGEwJV
SzEUMBIGA1UECBMLT3hmb3Jkc2hpcmUxETAPBgNVBACtCEFiaw5nZG9uMRYwFAYD
VQQKEw1CMk0gU29sdXRpb25zMRQwEgYDVQQLLEwtEZXZlbG9wbWVudDEUMBIGA1UE
AxMLRGV2ZWxvcG1lbnQwHhcNMTIwMzIwMTUzODQ5WhcNMzkwODA2MTUzODQ5WjB6
MQswCQYDVQQGEwJVSzEUMBIGA1UECBMLT3hmb3Jkc2hpcmUxETAPBgNVBACtCEFi
aw5nZG9uMRYwFAYDVQQKEw1CMk0gU29sdXRpb25zMRQwEgYDVQQLLEwtEZXZlbG9w
bWVudDEUMBIGA1UEAxMLRGV2ZWxvcG1lbnQwggEiMA0GCSqGSIb3DQEBAQUAA4IB
DwAwggEKAoIBAQDXxxsF1N+wliNk8YP3vcr3Im32995Lt5GC20XNYYF/
FrtgPB9WXS0DZOTVTYKpg7+EOJ9gwZK4MOvMH/
LTBSB7a7yx9jpsSbabUYMK+NL5JanNBzvV5uVZ2cgJNvd/
YPH6BrXuBODKaULaGydLdnIfeB/6rIvj4WCu37+6a+0vPwJSwEb9/
HfxAqm75nxOTNpwUdH+AgN49wZmd+WOhBaZB+JcmfPimkG/
9GQDisGf0c1YGOnTHHXpHIzrv1R6SGMAxm+/
xqnHoH1UPQGfLNOH4VKygGEOSrNTHIJtELXYISbuH3dYbRyzb5TMUd/
4WfmVabVi2ggP4VrhrncRhAgMBAAEwDQYJKoZIhvcNAQEFBQADggEBAGOrdDKLmV
bOuk8WrUY5/m8BC6ceSnsazYXs3s6CSpSTCqpKUpPkwc9LpP0pb2vHdJYzMDu/
oZHsfMFcwYHg7rMFf8/
tsLE0n0TKf2OfNSGpYNHRUEOCcYi9mUnLoondcV82K5nnuXsEaJ2OpSDwpp/
OVpo69+Ef8NA953xKAAGpSITNL3nOBftvRw3dMPhnEAzd7e5jX9an6JSjqU1h7Fb
asuhPVqixsKvuq6fqws/
jwFXeGNIig0hOVwvtUUWWJbvExo29pvq7pD4VQI5KN1BbwA6kKs6ueyl7tX5C/
FUZdKfoIfN6o97EAZ3DNBBkZtcvnnUUoBiMXmC60Ky6QNw=
```

Copy this text and paste into the Package Signing Certificate field as per step 2 above.

This method will auto-launch the Elemez app after installation.

The example below shows this configuration using 42Gears SureMDM platform.

The screenshot displays the 'Package Configuration' screen in the 42Gears SureMDM platform. The interface is organized into sections for configuring a package:

- Package Configuration:** The main header with 'Delete' and 'Add' icons.
- Package:** A section containing three input fields:
  - Class Name:** com.b2msolutions.elemez.activities.AutoEnrolmentActivity
  - Package Name:** com.b2msolutions.elemez
  - Package Signing Certificate:** MIIDcDCCAligAwIBAgIET2ikiTANBgkqhkiG9w0BAQUFADB6MQswCQYDVQQGEwJV
- Permissions:** A section with a '+ Add' button.
- Class Variances:** A section with a '+ Add' button.
- Feature Variances:** A section with a 'Delete' button and a '+ Add' button.
- Feature Variance:** A detailed view of a feature variance with the following configuration:
  - Variance Type:** Launch app after install/upgrade (selected from a dropdown menu)

## Enroll the Device

After you configure a profile to include the Elemmez application with its Managed Config, the Elemmez Zebra Extension and the Zebra Legacy OEMConfig app or Zebra OEMConfig Powered by MX app with its configuration profile, you can enroll a device into your estate using this profile.

Each device should:

- Be granted the runtime permissions it needs to operate.
- Auto-launch the Elemmez app silently after installation.

# SAMSUNG AGENT DEPLOYMENT

This chapter describes best practices for deploying the Elemez Android device agent to Samsung devices using a generic Android Enterprise model. It assumes familiarity with Android Enterprise, Managed Config, and OEMConfig methods.

## Deployment Guide

This section describes the steps required to deploy Elemez to Samsung devices using Android Enterprise methods.

## Prerequisites

This method requires that the Samsung device is running Android 13 or higher. You should not need to purchase a Knox Enterprise license or other additional Knox license to use the features described below.

This configuration has been tested on devices deployed in “Corporate-owned Dedicated Device” mode only. It requires a minimum version of 71300 for the Elemez agent.

## Deployment Method

There is no Elemez extension for Samsung devices. The following information will not be available in the Elemez platform when using the main agent only:

- Detailed battery information such as serial number, part number, health, etc. Instead, the battery charge level will be tracked at the device levels and metrics such as average discharge rate per hour will be presented for the device itself. As these devices do not have removable batteries, this should not be a concern.
- The SIM Serial Number is not retrievable from the device.

All other information should be collected and presented in Elemez as usual. The general steps for deploying Elemez to Samsung using an Android Enterprise platform are :

1. Add the Elemez app from the Google Play store or a Managed Play store to the EMM.
2. Add the Samsung Knox Service Plugin OEMConfig app from the Play store to the EMM.
3. Configure the Elemez app Managed Config information.
4. Configure the Samsung KSP OEMConfig profile to auto-launch the Elemez app, set permissions to allow data usage and app usage metrics to be collected, and to whitelist the app for battery optimization.
5. Send the apps and OEMConfig profile to the device. The app will auto-launch and register with the Elemez platform.

These steps are described further in this section.

1. Add the Elemez app from the Google Play store to the EMM.
2. Add the Samsung Knox Service Plugin (KSP) OEMConfig app to your EMM.
3. Configure the Elemez app. Create a profile for the Elemez App in the EMM. The app configuration profile must be set up as described below.
  - You must auto-grant the required runtime permissions for Elemez. You may be able to choose to auto-grant all permissions to the app or to auto-grant each requested permission independently, dependent upon the EMM platform in use.
  - In the Managed Config settings for the Elemez app, add a “Token” key (mandatory). The value for token is the “enrollment token” for your Elemez world, which you can find in your Elemez menu options or as provided by your Managed Services Provider.
  - In the Managed Config settings for the Elemez app, add a Serial Number key (mandatory). Elemez cannot read the serial number directly from the device; therefore, it must be provided to the agent from the EMM at deployment time. Most EMMs have a method to provide the serial number of the device as a wildcard in this configuration option. For example, 42Gears' SureMDM allows you to enter \$serialnumber\$ as a wildcard in Managed Config such that the actual value of the serial number will be provided to each device at deployment time.  
If the EMM is not able to provide the serial number, then it may be possible to substitute an alternative unique field, such as the IMEI. For example, Microsoft's Intune does not allow the serial number to be passed to the app, but does allow the IMEI to be passed through using the string {{IMEI}}. If this is the case then you may wish to differentiate this identifier from the actual IMEI by some method, such as surrounding the string with [ ], e.g. [{{IMEI}}]. It is critical that whichever value you choose to enter in this field, it must be unique across the estate as this is how Elemez differentiates your devices.
  - In the Managed Config settings for the Elemez app, add an IMEI key (optional). Similar to the serial number, many EMMs provide a method to

pass the IMEI as a wildcard through Managed Config. If this is not the case, then you may leave this field empty, and the IMEI will not be populated.

The examples below show how these settings may be configured using Microsoft's Intune UEM.

**Samsung Elemz Config | Properties**

Search

- Overview
- Manage
- Properties**
- Monitor
- Device install status

**Basics** Edit

Name: Samsung Elemz Config  
 Description: No Description  
 Device enrollment type: Managed devices  
 Platform: Android Enterprise  
 Profile Type: Fully Managed, Dedicated, and Corporate-Owned Work Profile Only  
 Targeted app: Elemz

**Settings** Edit

**Permissions**

| Permission                   | Permission state | Permission name            | Permission group |
|------------------------------|------------------|----------------------------|------------------|
| Phone state (read)           | Auto grant       | READ_PHONE_STATE           | PHONE            |
| External storage (write)     | Auto grant       | WRITE_EXTERNAL_STORAGE     | STORAGE          |
| External storage (read)      | Auto grant       | READ_EXTERNAL_STORAGE      | STORAGE          |
| Location access (background) | Auto grant       | ACCESS_BACKGROUND_LOCATION | LOCATION         |
| Location access (coarse)     | Auto grant       | ACCESS_COARSE_LOCATION     | LOCATION         |
| Location access (fine)       | Auto grant       | ACCESS_FINE_LOCATION       | LOCATION         |

**Configuration Settings**

| Configuration key | Value type | Configuration value                                    |
|-------------------|------------|--------------------------------------------------------|
| IMEI              | string     | {{IMEI}}                                               |
| Serial Number     | string     | {{IMEI}}                                               |
| Token             | string     | AqrFJdcljwhrjaaDeKmX/WapKDM8VmmNGUjMZGIC0zKIZZuazUC... |

4. Configure the relevant options in the KSP OEMConfig app and save the OEMConfig profile. The examples shown in this section are from the 42Gears SureMDM EMM *<do these examples apply?>* .
  - a. Enable device policy controls.
  - b. Add application management policies.
  - c. Add the launch activity.
  - d. Enable permission controls.
  - e. Configure permissions.
  - f. Save the OEMConfig profile.
5. After you have configured a profile to include the Elemz application with its Managed Config and the KSP OEMConfig app with its configuration profile, enroll the device into your estate using this profile.  
 Each device should:
  - Receive the usage access (PACKAGE\_USAGE\_STATS) permission for the Elemz app. You can check this through Settings / Apps / Elemz / three bars or dots / special access / usage data access. Elemz should be enabled automatically for this special permission.
  - Be granted the runtime permissions it needs to operate.
  - Be whitelisted for battery optimization.
  - Auto-launch the Elemz app silently after installation.



# WINDOWS AGENT INSTALLATION

This document describes how to install the Windows Agent.

## Check the Communications Path to the Elemenez Cloud Platform

Ensure that the devices on which the agent is to be installed are connected to a network that allows communication with the Elemenez cloud platform. If a firewall is in place, then configure the firewall to allow outbound connections to the appropriate Elemenez Data Center:

- UK: api.uk.elemenez.com (TCP:443) (52.56.219.238 & 18.130.19.143)
- US: api.elemenez.com (TCP:443) (54.83.18.223 & 54.83.18.250)

Note that the agent should automatically detect and use any forwarding proxy in the enterprise network. If communication through a proxy appears to not be working, contact Honeywell support.

## Download the Elemenez Agent for Windows

To enroll a device into Elemenez, you will need the latest version of the Elemenez Agent for Windows. This can be obtained from the following link:

<http://elemenez.com/downloads/client/x86/latest/ElemenezInstaller.msi>

You will also need a token file for your customer world. The token file informs the agent which Elemenez data center to enroll the device at and which world the device is associated with. Each device must have a copy of the token file prior to installing the Agent. The token file can be downloaded from your Elemenez UI.

1. From the menu option at the top of any Elemenez page, select **Enrollment**.
2. Use the button to download a copy of the elemenez.token file.
3. Copy the elemenez.token file to the c:\windows folder on the target device.

Note that the `elemez.token` file will be removed from this folder once the agent has successfully registered with the Elemez cloud.

## Install the Agent to Register the Device with the Cloud Service

To register for the service, you must install the Elemez agent on the device. You can typically do this using one of three methods:

- By downloading and silently installing the agent and the token file remotely via a unified endpoint management (UEM) platform such as Microsoft's Intune, or via a system management platform such as Microsoft Endpoint Configuration Manager (SCCM) or LANDesk.
- By running the MSI installer locally on the device.
- By adding the agent to a gold image and using that image to commission a new device.

Once the agent is installed, you will see the service icon in the Windows tray when the agent is actively running in the background. Right-click the icon and check the Status menu to confirm that the agent has successfully contacted the server and is in the state "Commissioned."

The device will appear in your Elemez world and the agent will continue to operate over a device reboot.

## Uninstalling the Agent

To uninstall the Windows agent, use your normal method for uninstalling a Windows application from the device. This can be done locally using the Windows interface or remotely using an MDM/EMM platform or other method.

# WINDOWS AGENT DEPLOYMENT WITH INTUNE

This document describes a method for how to deploy the Elemez Windows agent using Microsoft's Intune UEM and assumes some familiarity with the use of Intune to manage a Windows estate. Even if the method described in this guide may be well understood already, the full description for how to package and deploy Elemez is provided here for completeness.

## Note to Panasonic Smart Essentials Customers

The Smart Essentials service utilizes the B2M Elemez platform and Elemez Windows agent. Note that the information in this document applies equally to Elemez and Smart Essentials versions of the product and service.

## Deployment Guide

This section describes the generic steps required to set up Intune for an Elemez Windows agent deployment.

The steps necessary to achieve this are:

1. Download the Win32 App Content Prep Tool from Microsoft's website, the latest version of the Elemez Windows agent, and the token file for your Elemez world.
2. Create PowerShell scripts to deploy and move the token file to the c:\windows folder on the target device, to detect the presence of the token file, and to remove the token file.
3. Package the Elemez token file ready for Intune deployment.
4. Package the Elemez Windows agent ready for Intune deployment.
5. Add the Token File package to Intune.
6. Add the Elemez Windows Agent package to Intune with a dependency on the Token File package.
7. Assign the Token File package and Elemez Windows Agent package to the target device groups.

These steps are outlined in this section.

## Download the Required Utilities and Files

Download the Microsoft Win32 Content Prep Tool from here:

<https://github.com/microsoft/Microsoft-Win32-Content-Prep-Tool/blob/master/IntuneWinAppUtil.exe>

Download the latest Elemez Windows Agent from here:

<https://elemez.com/downloads/client/x86/latest/ElemeszInstaller.msi>

Download your Elemez Token. From the Elemez menu, select Enrollment, then download the token file to your local storage.

Create two new folders, one to hold the source files for the token file distribution and the other to hold the source files for the Elemez agent distribution. For this example we have used:

- c:\users\public\intune\elemesz\_token\_files
- c:\users\public\intune\elemesz\_agent\_files

Add the elemesz.token file into the c:\users\public\intune\elemesz\_token\_files folder.

Add the ElemeszInstaller.msi file into the c:\users\public\intune\elemesz\_agent\_files folder.

## Package the Elemez Token File for Deployment

This method puts a file onto the target PC by treating the file as a Win32 application with PowerShell commands for install and uninstall.

### Create PowerShell Scripts

1. Create two PowerShell scripts:

Install-Token-File.ps1

```
Move-Item -Path "$PSScriptRoot\elemesz.token" -Destination
"$Env:windir\elemesz.token"
if (test-path -path "$Env:windir\elemesz.token") {
    exit 0
}
else { exit 1 }
```

#### Remove-Token-File.ps1

```
if (Test-Path -Path "$Env:windir\elemesz.token") {  
  Remove-Item -Path "$Env:windir\elemesz.token"  
}  
if (Test-Path -Path  
"$Env:programdata\biz2mobile\elemesz\elemesz.token") {  
  Remove-Item -Path  
"$Env:programdata\biz2mobile\elemesz\elemesz.token"  
}  
exit 0
```

2. Add the files to the c:\users\public\intune\elemesz\_token\_files folder.
3. Create a PowerShell script file called Detect-Token-File.ps1 and store it in a separate folder:

```
if ((Test-Path -Path "$Env:windir\elemesz.token") -or (Test-Path -  
Path "$Env:programdata\biz2mobile\elemesz\elemesz.token")) {  
  Write-Host "elemesz.token file detected"  
  exit 0  
} else {  
  Write-Host "elemesz.token file not detected"  
  exit 1  
}
```

4. Create the Elemez Token File Deployment Package.  
Create the Intune Elemez token file package using the Microsoft Win32 Content Prep Tool with this command line:

```
IntuneWinAppUtil.exe -c  
"c:\users\public\intune\elemesz_Token_Files" -s "elemesz.token" -o  
"c:\users\public\intune\intune_elemesz_token" -q
```

This will create a file called elemesz.intunewin in the  
c:\users\public\intune\intune\_elemesz\_token folder.

## Package the Elemez Agent for Deployment

Create the Intune Elemez Windows agent package using the Microsoft Win32 Content Prep Tool with this command line method:

```
IntuneWinAppUtil.exe -c  
"c:\users\public\intune\elemesz_Agent_Files" -s  
"ElemeszInstaller.msi" -o  
"c:\users\public\intune\intune_elemesz_agent" -q
```

This will create a file called elemeszInstaller.intunewin in the  
c:\users\public\intune\intune\_elemesz\_agent folder.

## Add the Elemez Token File Package to Intune

1. In Intune, create a new Windows App.
2. Select Win32 as the app type.
3. Add the Elemez Token File package file from the c:\users\public\intune\intune\_elemez\_token folder.
4. Complete the App Information panel by entering “B2M Solutions” as the Publisher and 1.0 as the App Version.
5. Complete the App Program panel. Use the following strings for the Install Command and Uninstall Command.

Install Command:

```
%windir%\system32\windowspowershell\v1.0\powershell.exe -  
executionpolicy bypass -file "Install-Token-File.ps1"
```

Uninstall Command:

```
%windir%\system32\windowspowershell\v1.0\powershell.exe -  
executionpolicy bypass -file "Remove-Token-File.ps1"
```

- Set the installation time to 1 minute, the install behavior to “System” and the device restart behaviour to “No Specific Action”.
6. Complete the Requirements Panel. Set the minimum Windows version for the package.
  7. Complete the Detection Rules panel. Set the “Rules Format” to “Use a custom detection script” and select the script file as the “Detect-Token-File.ps1” script that you created and saved earlier.

Complete the rest of the panels, but do not assign the app to any groups yet.

## Add the Elemez Agent Package to Intune

1. In Intune, create a new Windows App.
2. Select Win32 as the app type.
3. Add the Elemez Agent package from the c:\users\public\intune\intune\_elemez\_agent folder.
4. Complete the App Information Panel by setting “B2M Solutions” as the Publisher.
5. Complete the Program panel. Set the “Installation time required (mins)” field to 5. Set the “Device restart behavior” field to “No specific action”.
6. Complete the Requirements panel. Set the “Minimum operating system” field as appropriate.
7. Complete the Detection Rules panel. Use “Manually configure detection rules” and choose the MSI code as the detection method.
8. Complete the Dependencies panel. This will ensure that the elemez.token file has been deployed to the PC prior to deploying the Elemez App. If not, then the

system will force the deployment of the `elemez.token` file prior to installing the Elemez App.

9. Skip through the remaining panels and create the app package without assigning the app to any groups.

## Deploy the Token File and Elemez Apps

To deploy Elemez to your devices:

1. Assign the Token File app to your target group.
2. Assign the Elemez Agent app to your target group.

## Updating the Elemez Agent

To update the agent version in the field use the following instructions.

### Upgrading the Agent to a Later Release

These instructions are to upgrade the Elemez Agent app package in the field to a later release.

1. Create a new Win32 app package for the new Elemez agent release.
2. Add the new package into Intune.
3. Configure the Supersedence settings such that the new agent supersedes any of the earlier versions installed across the estate.
4. Save the package and assign it to the target groups where the app update is required.

While it is not necessary to uninstall the previous version on an upgrade, you can choose to do so if this is preferred. Note that in this case, you will lose information collected but not yet reported to the server by the previous agent on the device. This will typically be less than one hour of data in cases where the device is in regular contact with the Elemez server.

### Downgrading the Agent to an Earlier Release

These instructions are to downgrade the Elemez Agent in the field to an earlier release.

1. Create a Win32 app package for the earlier Elemez agent release.
2. Add the package into Intune.
3. Configure the Supersedence settings such that the earlier agent supersedes the later versions installed across the estate.

4. Save the package and assign it to the target groups where the app downgrade is required.

In this case it is required that you uninstall the later version of the agent on a downgrade. This is because database changes in the earlier version may not be compatible with the database schema on the later version. You will lose any information collected but not yet reported to the server by the previous agent on the device. This will typically be less than one hour of data in cases where the device is in regular contact with the Elemex server.

# WINDOWS AGENT DEPLOYMENT WITH SCALEFUSION

This chapter describes how to deploy the Windows agent using Scalefusion.

## Agent Deployment

1. Download the latest Agent from:  
<http://elemez.com/downloads/client/x86/latest/ElemezInstaller.msi>
2. Retrieve a token.
  - a. From any page on the dashboard, click on your username in the top right corner and select Enrollment.
  - b. A Token String is displayed. This can be locally saved by clicking on the download icon. By default, the filename is elemez.token. Save the elemez.token file downloaded and note its location.
3. Using the Scalefusion Deployer Application, build the package that will deploy Elemez and the token to a device.
  - a. Click Select Files and add both the token file and ElemezInstaller.msi.
  - b. Change the Extraction Folder Path to C:\ProgramData\Biz2Mobile\Elemez.
  - c. Select the ElemezInstaller.msi and click “Properties”.
  - d. Enter the Command Line Arguments.
    - /qn or /quiet for no ui or user interaction during install (silent install)
    - Add additional arguments as desired
  - e. Keep Execution Context set to “Device Level” and click “Save”.
  - f. Click “Compile SFX Exe”.  
Note the location you save the EXE file.
4. Add the Elemez application in Scalefusion.
  - a. Click on Application Management\Enterprise Store and Upload a New Windows App.
  - b. For the Application Type, select “EXE”.
  - c. Enter the Display Name and the current version. Upload a logo (optional).

- d. Select "Upload the same app for 64 & 32 bit" and select the EXE file you compiled in previous steps.
- e. For App Arguments use the following:
  - App Installation Mode: Run as Background
  - Installation Target: Device Level
  - Installation Argument: /quiet
  - Uninstallation Path: C:\Windows\System32\msiexec.exe
  - Uninstallation Arguments:  
/uninstall "C:\ProgramData\Biz2Mobile\Elemez\ElemezInstaller.msi" /qn /L\*  
"C:\elemezuninstall.log"
- f. For App Detection Rules, use the following:
  - Installation Detection Rule: File Exists
  - Installation Detection Path:  
C:\Program Files (x86)\Biz2Mobile\Elemez\Elemez.exe
- g. Click Save.
- h. Publish to the Group you wish to deploy to.
- i. On a target device, you can tell if the install was successful by looking for the Elemez Icon in the System Tray. If you right click "Status," the device should say Commissioned.  
The device should also appear in the Devices list in the Elemez Console.



Honeywell  
855 S. Mint Street  
Charlotte, NC 28202

[automation.honeywell.com](http://automation.honeywell.com)