



Getting Started

/ Identity Edge Controller 6.5

Latest update: 6.5

Lana Frost

ForgeRock AS.
201 Mission St., Suite 2900
San Francisco, CA 94105, USA
+1 415-599-1100 (US)
www.forgerock.com

Copyright © 2019 ForgeRock AS.

Abstract

Guide to getting started quickly with ForgeRock® Identity Edge Controller software.



This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivs 3.0 Unported License.

To view a copy of this license, visit <https://creativecommons.org/licenses/by-nc-nd/3.0/> or send a letter to Creative Commons, 444 Castro Street, Suite 900, Mountain View, California, 94041, USA.

ForgeRock® and ForgeRock Identity Platform™ are trademarks of ForgeRock Inc. or its subsidiaries in the U.S. and in other countries. Trademarks are the property of their respective owners.

UNLESS OTHERWISE MUTUALLY AGREED BY THE PARTIES IN WRITING, LICENSOR OFFERS THE WORK AS-IS AND MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND CONCERNING THE WORK, EXPRESS, IMPLIED, STATUTORY OR OTHERWISE, INCLUDING, WITHOUT LIMITATION, WARRANTIES OF TITLE, MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NONINFRINGEMENT, OR THE ABSENCE OF LATENT OR OTHER DEFECTS, ACCURACY, OR THE PRESENCE OF ABSENCE OF ERRORS, WHETHER OR NOT DISCOVERABLE. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES, SO SUCH EXCLUSION MAY NOT APPLY TO YOU.

EXCEPT TO THE EXTENT REQUIRED BY APPLICABLE LAW, IN NO EVENT WILL LICENSOR BE LIABLE TO YOU ON ANY LEGAL THEORY FOR ANY SPECIAL, INCIDENTAL, CONSEQUENTIAL, PUNITIVE OR EXEMPLARY DAMAGES ARISING OUT OF THIS LICENSE OR THE USE OF THE WORK, EVEN IF LICENSOR HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

DejaVu Fonts

Bitstream Vera Fonts Copyright

Copyright (c) 2003 by Bitstream, Inc. All Rights Reserved. Bitstream Vera is a trademark of Bitstream, Inc.

Permission is hereby granted, free of charge, to any person obtaining a copy of the fonts accompanying this license ("Fonts") and associated documentation files (the "Font Software"), to reproduce and distribute the Font Software, including without limitation the rights to use, copy, merge, publish, distribute, and/or sell copies of the Font Software, and to permit persons to whom the Font Software is furnished to do so, subject to the following conditions:

The above copyright and trademark notices and this permission notice shall be included in all copies of one or more of the Font Software typefaces.

The Font Software may be modified, altered, or added to, and in particular the designs of glyphs or characters in the Fonts may be modified and additional glyphs or characters may be added to the Fonts, only if the fonts are renamed to names not containing either the words "Bitstream" or the word "Vera".

This License becomes null and void to the extent applicable to Fonts or Font Software that has been modified and is distributed under the "Bitstream Vera" names.

The Font Software may be sold as part of a larger software package but no copy of one or more of the Font Software typefaces may be sold by itself.

THE FONT SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF COPYRIGHT, PATENT, TRADEMARK, OR OTHER RIGHT. IN NO EVENT SHALL BITSTREAM OR THE GNOME FOUNDATION BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, INCLUDING ANY GENERAL, SPECIAL, INDIRECT, INCIDENTAL, OR CONSEQUENTIAL DAMAGES, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF THE USE OR INABILITY TO USE THE FONT SOFTWARE OR FROM OTHER DEALINGS IN THE FONT SOFTWARE.

Except as contained in this notice, the names of Gnome, the Gnome Foundation, and Bitstream Inc., shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Font Software without prior written authorization from the Gnome Foundation or Bitstream Inc., respectively. For further information, contact: fonts at gnome dot org.

Arev Fonts Copyright

Copyright (c) 2006 by Tavmjong Bah. All Rights Reserved.

Permission is hereby granted, free of charge, to any person obtaining a copy of the fonts accompanying this license ("Fonts") and associated documentation files (the "Font Software"), to reproduce and distribute the modifications to the Bitstream Vera Font Software, including without limitation the rights to use, copy, merge, publish, distribute, and/or sell copies of the Font Software, and to permit persons to whom the Font Software is furnished to do so, subject to the following conditions:

The above copyright and trademark notices and this permission notice shall be included in all copies of one or more of the Font Software typefaces.

The Font Software may be modified, altered, or added to, and in particular the designs of glyphs or characters in the Fonts may be modified and additional glyphs or characters may be added to the Fonts, only if the fonts are renamed to names not containing either the words "Tavmjong Bah" or the word "Arev".

This License becomes null and void to the extent applicable to Fonts or Font Software that has been modified and is distributed under the "Tavmjong Bah Arev" names.

The Font Software may be sold as part of a larger software package but no copy of one or more of the Font Software typefaces may be sold by itself.

THE FONT SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF COPYRIGHT, PATENT, TRADEMARK, OR OTHER RIGHT. IN NO EVENT SHALL TAVMJONG BAH BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, INCLUDING ANY GENERAL, SPECIAL, INDIRECT, INCIDENTAL, OR CONSEQUENTIAL DAMAGES, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF THE USE OR INABILITY TO USE THE FONT SOFTWARE OR FROM OTHER DEALINGS IN THE FONT SOFTWARE.

Except as contained in this notice, the name of Tavmjong Bah shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Font Software without prior written authorization from Tavmjong Bah. For further information, contact: tavmjong @ free . fr.

FontAwesome Copyright

Copyright (c) 2017 by Dave Gandy, <https://fontawesome.com/>.

This Font Software is licensed under the SIL Open Font License, Version 1.1. See <https://opensource.org/licenses/OFL-1.1>.

Table of Contents

Preface	iv
1. Overview of Identity Edge Controller Components	1
IEC Components	1
IEC Architecture	2
Using the IEC Training Environment	4
2. Contributing to the IEC Project	5
Contributing to the IEC Core	5
Finding and Logging Issues on IEC	5
IEC Glossary	6

Preface

Use this guide to understand what Identity Edge Controller (IEC) software can do and how you can contribute to the IEC open source project.

Chapter 1

Overview of Identity Edge Controller Components

The ForgeRock Identity Edge Controller (IEC) includes multiple components working together to enable devices to register as identities in ForgeRock Access Management (AM).

When a device has registered, the IEC enables that device to do the following:

- Obtain a configuration from AM
- Request OAuth2 access and ID tokens
- Be paired with a user, using the OAuth2 Device Flow
- Call customisable scripts in AM

IEC Components

The IEC includes the following components:

IEC Service

The IEC Service runs on an edge gateway on the local network and provides secure communications between client applications and AM.

The ARM TrustZone enabled version of the IEC Service provides secure storage on edge gateways that support OP-TEE.

IEC AM Plugin

The IEC AM Plugin adds IoT-specific functionality to AM and provides a secure communication point for the IEC Service into AM. The plugin enables the IEC Service to perform tasks such as registering edge nodes and retrieving OAuth2 tokens.

Edge Identity Manager

The Edge Identity Manager is a basic User Interface to AM that enables you to view and manage edge node identities.

IEC SDK Client Library

The SDK client library provides a simple C API for client applications to invoke AM functionality through the IEC Service. The SDK library is small and uses a secure lightweight messaging protocol so that it can run on constrained devices.

The following diagram shows the IEC components and where they are situated in an IoT system:

IEC Architecture

The IEC implements a hierarchy of nodes at the *edge*, typically, devices that run embedded software. Edge nodes are physical or virtual things that exist at the edge and benefit from having an identity. The nodes can range from *constrained nodes* that have tight limits on power, memory, and processing resources, to fully capable nodes that can connect securely across a wide-area network.

A node's *type* is stored with its identity and is used to make decisions about the node's functions and properties. In IEC, an edge node can be one of the following types:

- **IEC**

The IEC edge node type represents an IEC Service and has a one to many relationship with CLIENT edge nodes.

- **CLIENT**

The CLIENT edge node type represents a client application that uses the IEC SDK and has a one to many relationship with DEVICE edge nodes.

- **DEVICE**

The DEVICE edge node type represents a physical device that can be onboarded through the IEC SDK.

The following diagram shows the IEC architecture and the different node types:

Using the IEC Training Environment

In addition to this documentation on Backstage, the IEC project includes a training environment that enables you to get all the IEC components up and running very quickly in Docker containers, and to test your client applications.

The training environment includes a number of sample applications, referenced in the [Client Application Developers Guide](#).

Chapter 2

Contributing to the IEC Project

This chapter shows you how to get started contributing to the IEC project, where to find the IEC source code, and how to view and raise issues.

Contributing to the IEC Core

The IEC Core is an open source project that contains the source code and build instructions for the IEC edge components. The edge components include the following:

- IEC Service
- IEC SDK
- IEC Utility

The [IEC Core repository](#) is publicly available to browse or clone. ForgeRock customers and partners can contribute to the project if they have a *subscription agreement* with ForgeRock.

For information about obtaining a subscription agreement, see this [Knowledge Base article](#).

Finding and Logging Issues on IEC

The IEC core development is tracked at <https://bugster.forgerock.org/jira/projects/OPENIEC/issues>. You can browse the existing issues without logging in. If you have a customer or partner agreement with ForgeRock, you can log in to create new issues. Otherwise, contact the IoT team to create an issue on your behalf.

IEC Glossary

Access Management (AM)	ForgeRock software (part of the ForgeRock Identity Platform) that provides access and identity management.
client	An <i>edge node</i> type representing a client application that uses the IEC SDK.
constrained device	A device that does not have the ability to connect securely across wide-area networks, due to cost and/or physical constraints. See RFC 7228.
device	An <i>edge node</i> type representing a physical device that can be onboarded via a client node.
Directory Services (DS)	ForgeRock software that is part of the ForgeRock Identity Platform and provides storage for identities and configuration.
edge	Industry term for the geographic distribution of IoT devices. <i>Edge computing</i> enables a connected device to process data closer to where it is created (on the <i>edge</i>).
edge gateway	Hardware and software deployed at the <i>edge</i> , through which devices communicate.
Edge Identity Manager	ForgeRock software that provides a User Interface to AM for viewing and managing device identities.
edge node	A physical or virtual object that exists at the <i>edge</i> and benefits from having an identity. Examples of edge nodes include a device, the IEC Service or a client application.

Identity Edge Controller (IEC)	ForgeRock software consisting of multiple components that securely provide devices with identity.
IEC AM Plugin	ForgeRock software plugin that adds IoT specific functionality to AM.
IEC SDK	ForgeRock client library that provides an API for client applications to invoke AM functionality via the IEC Service .
IEC Service	ForgeRock software that runs on the edge gateway and provides secure communication between client applications and AM.
IEC Utility	ForgeRock software used when installing the IEC Service or IEC SDK to configure the components.
OP-TEE	Open source implementation of the GlobalPlatform Trusted Execution Environment (TEE) specification.
Rich Execution Environment (REE)	GlobalPlatform term for the environment in which the user-facing operating system runs.
Rich OS	Operating system running in the Rich Execution Environment (REE) , typically Linux.
Trusted Application (TA)	An application that can run in the Trusted Execution Environment (TEE) .
Trusted Execution Environment (TEE)	GlobalPlatform term for a secure area of the main processor of a device that ensures data is stored and processed in an isolated and trusted environment.