The Resilient Access Administrative Console provides graphical user interface (GUI) controls for adding and configuring custom authorities that perform an access control function. The authorities are grouped in the following categories:

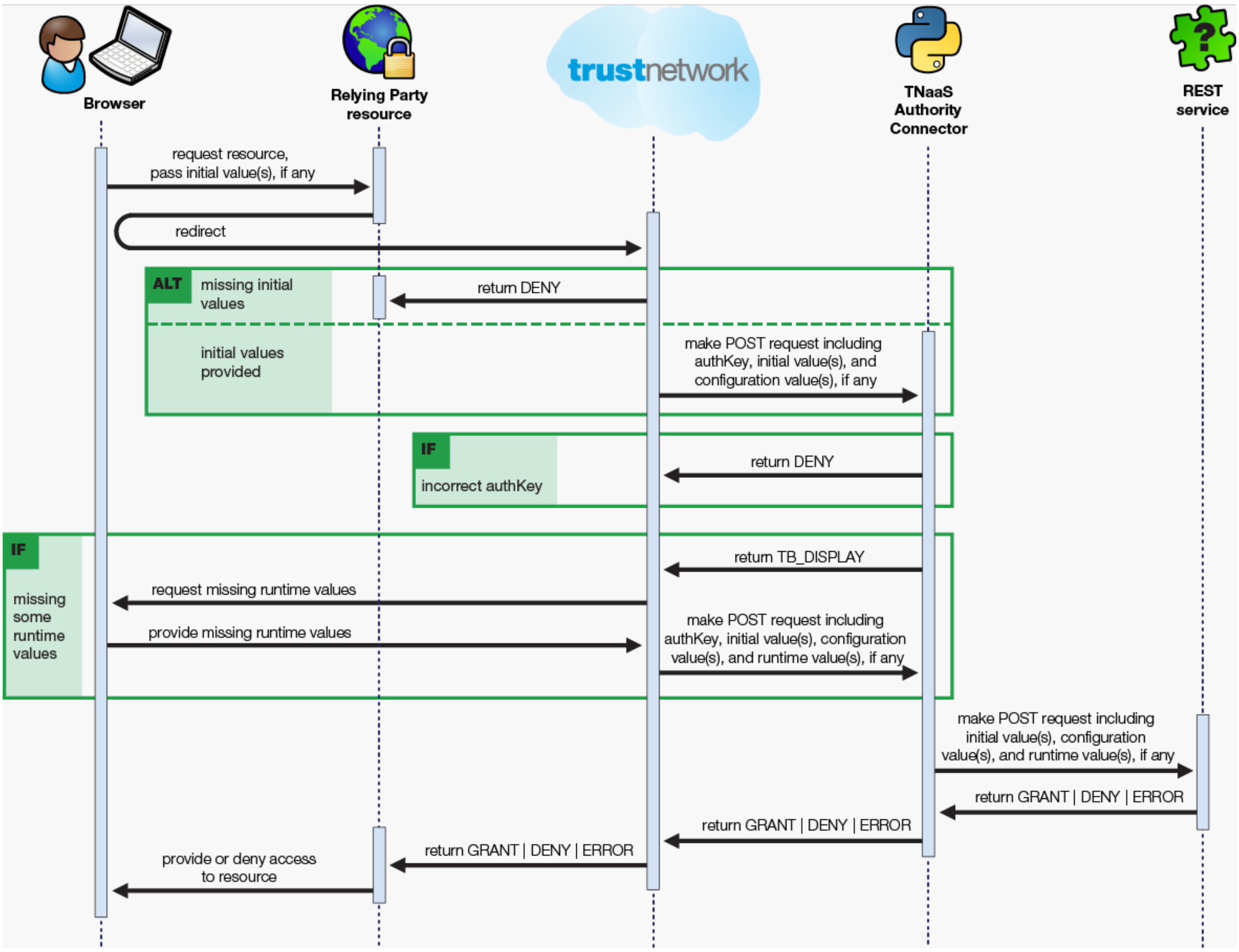
- **Authentication authorities:**This type of authority performs username/password authentication. Intensity Analytics typing cadence can be combined with these authentication authorities for an additional factor besides the verification of the password entered.
- **Authorization authorities:**This type of authority performs authorization function such as membership in an LDAP/AD Group for role based authorization or the evaluation of an expression consisting of the attributes passed to the authority. Another category of authorization authority integrates with XACML Rules engine for customers to integrate their Policy Decision Point (PDP) with an overall access policy configured in RA.
- **Policy Authority**This type of authority extracts identity attributes from a user's record and passes them as inputs to authorities in another policy E.g. retrieving a user's phone number from an Active Directory and performing 2nd factor SMS or phone authentication. This is the mechanism through which Resilient policy can be configured to dynamically expand to more complex policies, given a small set of initial identity attributes (e.g. email or user ID), retrieve other identity attributes and perform additional authentication/verification functions.
- **Attribute Provider authorities**This type of authority extracts identity attributes out of an Identity Store and returns them as a part of the policy result. For SAML these attributes are part of the SAML assertion and for OpenID Connect are part of the user claims.
- **Policy Composition Authorities** These type of authorities are typically used to create adaptive access policies e.g. if a user is accessing an application within the organization's network, a simple password authentication policy is sufficient. If accessing the application from VPN then a 2 factor authentication policy must be applied. If accessing from a public wifi, then a more robust authentication policy must be imposed.

Authority Connector

Since an organization's identity store is usually never exposed outside of the organization's internal network, the LDAP/AD or Database authorities have two parts, a service that executes in the deployment of the Resilient Access Management system, usually hosted in the cloud and an Authority Connector service, a lightweight HTTP service that runs on a server within the organization's network and connects to the identity store. The hosted authority service connects with the Authority Connector over a secure protocol and only performs query functions for authentication and identity attribute retrieval.

The Resilient Access Authority Connector bundle consists of a few scripts, a lightweight python web server, and an encrypted file containing the configuration information specified in the GUI. With no need for a database and its own web server, the Resilient Access Authority features a very small footprint, making it easy for authority providers to extract and run the Resilient Access Authority Connector inside their own environments. Through this mechanism customer's backend resources such as LDAP/Active Directory, Databases can remain behind the firewall with the Resilient Access Authority Connector taking responsibility for communications with Resilient Access through a secure interface that is based on key exchanges over TLS.

The following diagram illustrates the runtime sequence.


Browser
Relying Party resource
trustnetwork
TNaaS Authority Connector
REST service
request resource, pass initial value(s), if any
redirect
ALT
missing initial values
return DENY
initial values provided
make POST request including authKey, initial value(s), and configuration value(s), if any
IF
incorrect authKey
return DENY
IF
missing some runtime values
return TB_DISPLAY
request missing runtime values
provide missing runtime values
make POST request including authKey, initial value(s), configuration value(s), and runtime value(s), if any
make POST request including initial value(s), configuration value(s), and runtime value(s), if any
return GRANT | DENY | ERROR
return GRANT | DENY | ERROR
return GRANT | DENY | ERROR
provide or deny access to resource

The steps to create a new authority and make it available for use in policies are:

1. Create and configure the Authority in Resilient Access Admin console as explained below for each of the different authority types.
2. Download and deploy the Resilient Access Authority Connector. if applicable
3. Execute Resilient Access Authority tests to make sure the authority is configured correctly.
4. Turn the authority online, it will now appear in the Authority selection panel in the Policy creation page under your organization's authorities section.

The following types of Authorities are supported in Resilient Access at this time:

Authentication Authorities

- Custom REST Authentication

- LDAP/AD Authentication
- Database Authentication

Authorization Authorities

- LDAP/AD Group Membership
- Attribute Authorization

Policy Authorities

- Custom REST Policy Authority
- LDAP/AD Policy Authority
- Database Policy Authority

Attribute Provider Authorities

- Custom REST Attribute Provider
- LDAP/AD Attribute Provider
- Database Attribute Provider

Policy Composition Authorities

- Simple Policy Authority
- Decision Authority