CrashplanIDG

This documentation will help you integrate your identity services with CrashPlan offered by Code42 through Internet2's NET+ program. Associated portions of the NET+ Identity Guidance for Services are noted by section.

Discovery and Authentication

The CrashPlan client is configured to communicate with a backup server per a configuration file, and the backup server is in turn configured to point to the IdP. This configuration file can be distributed by an organization to its users by including it as part of a package. Session initiation is performed by accessing the SP, which then issues a SAML 2.0 AuthnRequest to the user to be delivered to the IdP(1.1.2).

Users must select upon initial application invocation that they would like to use an "Existing Account". Users must then select a checkbox labeled "Login with Single-Sign-On" and enter credentials for authentication. The client acts as a web browser and performs the actual authentication transaction, delivering the assertion to the organization's CrashPlan server.

Each CrashPlan PROe server can only use a single identity provider at this time.

Attributes

CrashPlan expects to receive a username similar to `uid`. The below are the default SAML attribute mappings to attributes as understood by CrashPlan.

CrashPlan Attribute	Recommended SAML Attribute Name	Optional
username	urn:oid:0.9.2342.19200300.100.1.1	No
firstname	urn:oid:2.5.4.42	Yes
lastname	urn:oid:2.5.4.4	Yes
email	urn:oid:0.9.2342.19200300.100.1.3	Yes

The server administrator can customize the mappings of SAML attribute name to CrashPlan attribute.

Privileges

Any user that can authenticate to the IdP is considered eligible for backup service through CrashPlan. Organizational membership can be configured in the administrative interface, but not mapped by user attribute.

Authentication to the administrative portions of the CrashPlan server and its web interface can be performed using single sign-on or direct authentication, either independently configured of authentication for backup clients.

Provisioning

Provisioning of users to the CrashPlan server can happen dynamically in the front channel during the installation of CrashPlan client software or can be done in bulk using an administrative interface or by use of bulk export formats such as CSV's.

Deprovisioning

Users must be manually deprovisioned by administrators using the CrashPlan application.

Logout

The application portion of CrashPlan, because it is a continuously running backup system, doesn't support logout. The web interface for CrashPlan does allow users to log out of the web interface itself.

Implementation

The PROe server has a native SAML SP implementation. Shibboleth was the reference implementation used for the development of this SP.

Metadata Support

The PROe server publishes automatically generated metadata about itself at a URL that the identity provider can use, though manual editing of that metadata file may be required in some instances. The SP will load identity provider metadata from a URL configured by the PROe server administrator.

Non-Browser Access

Most of the CrashPlan service is a native application running on users' machines, and this service is authenticated by emulating a web browser for the login flow.

Example Configuration for SAML Implementations

Interoperability has been demonstrated against Shibboleth, PingFederate, and Okta.