forsyte
PIM EXTENDER

PIM Extender

EXTEND YOUR JUST-IN-TIME ADMIN CAPABILITIES FROM CLOUD TO ON-PREMISE WITH EASE

forsyte PIM EXTENDER

Manage, control, & monitor just-in-time access to your organization's important resources & operational activities, & secure user access rights with the click of a button.

What is PIM Extender?

PIM Extender is a SaaS based offering provided by Forsyte I.T. Solutions that is designed to enhance the functionality of Azure's Privileged Identity Manager (PIM) offering by extending it to your on-premise Active Directory. As you work to enhance the capabilities of your technology, PIM Extender empowers you to take control of Azure functionality.

Experience the Benefits of PIM Extender:

- Minimal deployment & set up time
- Time bound access to privileged accounts
- Unified Just-In-Time administration experience across hybrid environments
- Lower attack surface by implementing Just-In-Time administrative principals
- Low TCO

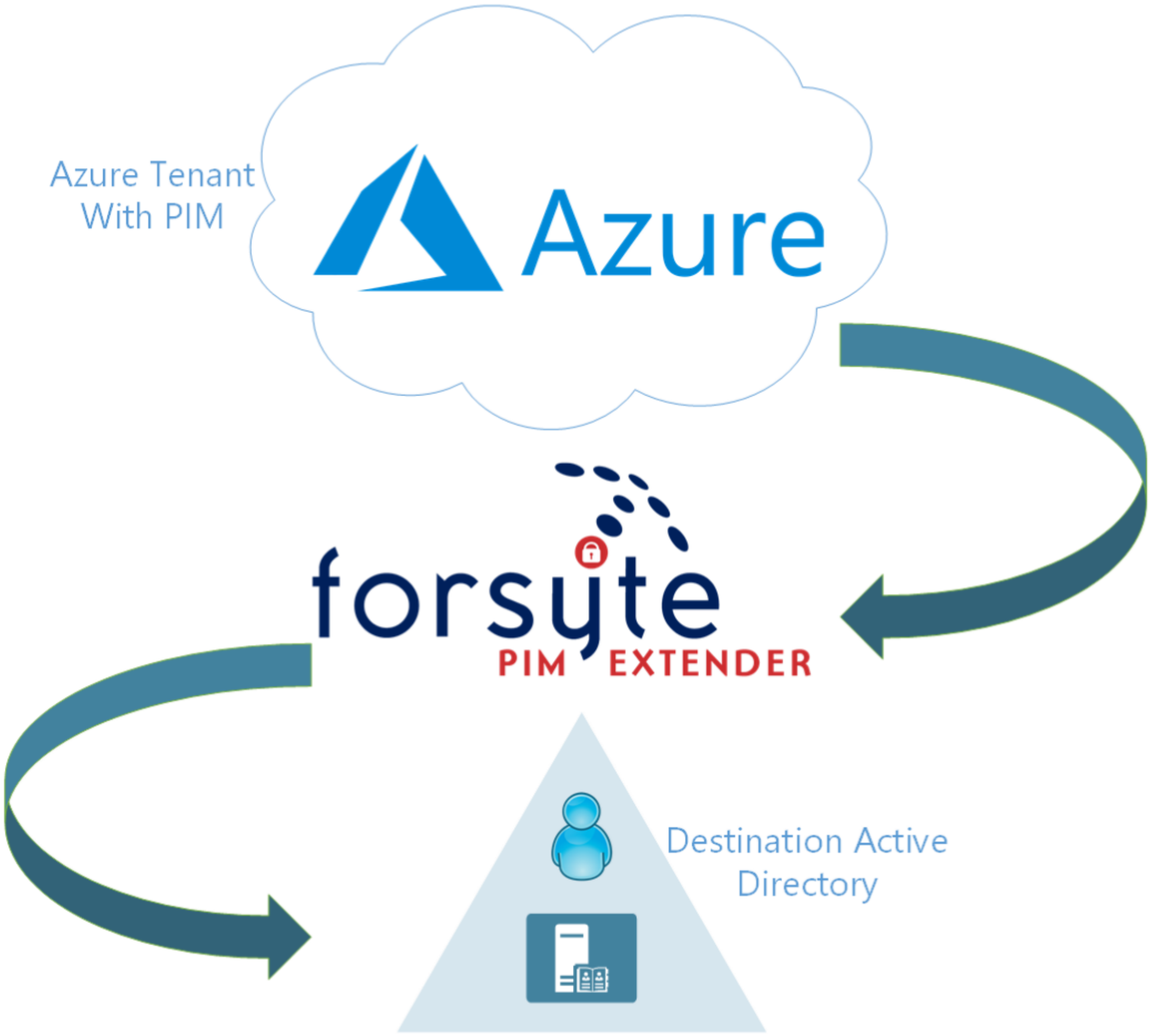
PIM Named a Top 10 Security Project for 2019 by Gartner Research

"Verizon's 2018 Data Breach Investigations Report reveals that 63% of security incidents within 2017 were attributed to compromise of unprotected privileged accounts." - Verizon Enterprise

Identity Governance that works for you.

Powered by: forsyte I.T. SOLUTIONS

Connectivity Diagram



Technical Description

This solution is cloud based bringing the scalability and security of Microsoft Azure to your on-premises data center.

The following sections outline technical details of the PIM Extender offering.

Workflow

1. Map a Azure AD Custom role to one or more on-premises Active Directory groups
2. The PIM Extender service constantly monitors your Azure AD
3. When an eligible user is given access to a role with a mapping rule, PIM Extender captures this event
4. The service encrypts the relevant information and adds it to a queue for collection
5. The registered on-premises service picks up the request and decrypts the information
6. The on-premises agent then adds the user to the proper Active Directory group, setting the group membership TTL

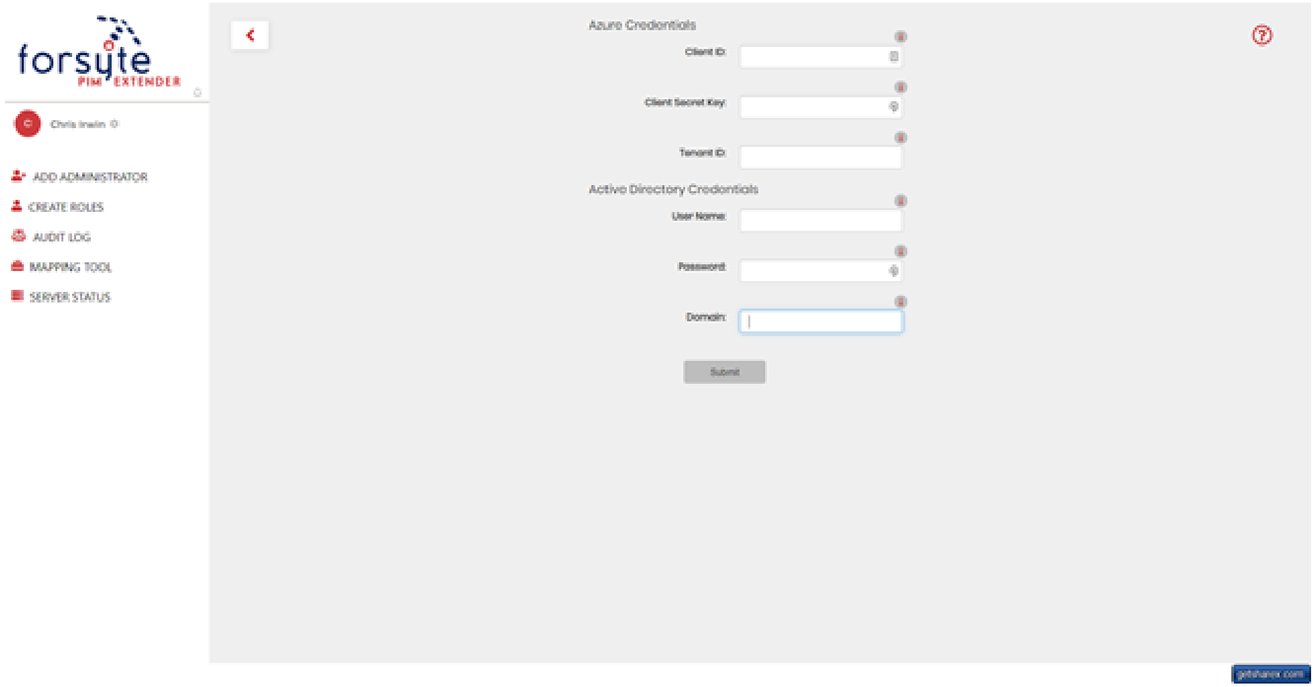
Security

- All sensitive data (Application ID's, Keys, etc.)
- is encrypted and then stored in FIPS 140-2
- Level 2 compliant Hardware Security Modules (HSMs)
- All communications are encrypted using SSL/TLS 1.2
- All data synchronizations happen in memory to ensure that no user information is stored in our databases
- Any data is encrypted in transit and at rest

Set Up

Credentials

The first time you access the PIM Extender solution you will be presented with a screen to enter the needed connection information:



The following needs to be provided for your two accounts:

- The first is an account for the management of Azure
- The second is an Active Directory account to provide group management

Azure

An application account is needed for the PIM Extender service to create custom Azure roles as well as to detect when the role has been assigned. If you need directions on how to create this account, please click here for additional assistance. Once you have registered an application account please collect and provide the following:

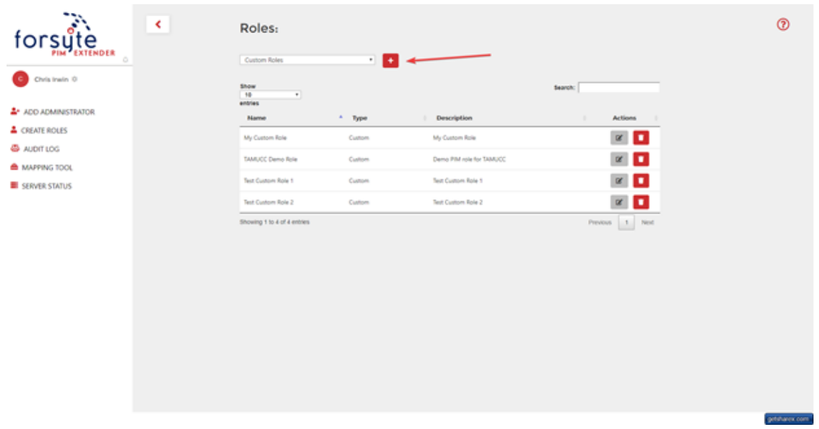
- Application Client ID
- Application Client Key
- Azure Tenant ID

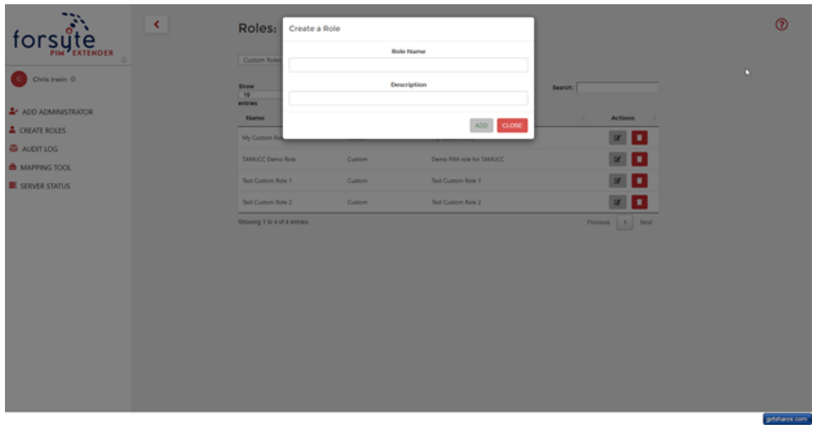
Active Directory

A service account is required that has rights to manage groups in the selected OU. This account will be used to discover OU's and add users to the mapped group. *Please note that you will not be able to view any additional options until you have supplied the needed onnection information.

Azure AD Custom Roles

Azure Active Directory (AAD) now offers the ability to create custom roles. These roles can be used to assign a wide verify of Azure specific rights. PIM Extender takes advantage of this feature by creating an association with a security group in the on premises Active Directory.
You can follow the traditional creation path detailed here or you can utilize the "Create Role" feature in the PIM Extender tool:

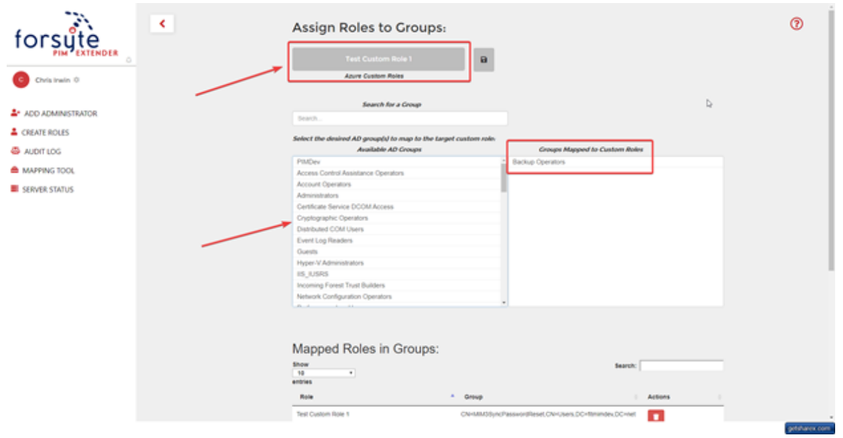




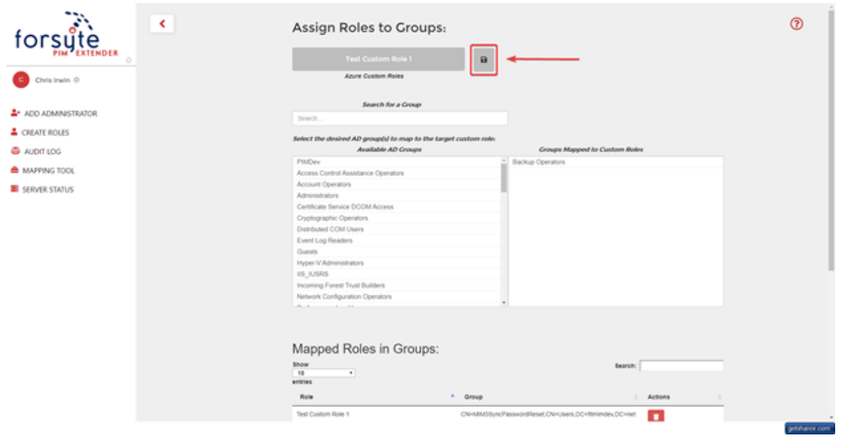
Azure Custom Role Mapping

The final step is to create a mapping between the Azure custom role and the on-premises group(s).

- First, select a custom role then select one or more groups to map it to:



- After you have made your selections click the small disk to save the changes:



PIM Extender revolutionizes the way your organization is able to manage Identity Governance & takes the guesswork out of accessing Azure functionality within your on-premise environments.

forsyte PIM EXTENDER

PIM Extender revolutionizes the way your organization is able to manage Identity Governance & takes the guesswork out of accessing Azure functionality within your on-premise environments.

Working together, you will be empowered to do more:

- Single User Tracking
- Admin User Tracking
- Managed User Lifecycle

- Unified JIT Administration
- JIT Security
- Just Enough Administration

Identity Governance that works for you.

Microsoft Gold Partner

- Contact Us or Your Microsoft Account Executive to Get Started.

FORSYTEIT.COM | CONTACT@FORSYTEIT.COM | 844.587.4535 | @FORSYTEIT

Powered by: forsyte I.T. SOLUTIONS