Integración con los protocolos del servidor de correo de Microsoft Office 365

Integración con los protocolos del servidor de correo de Microsoft Office 365

Volver al índice de documentación de Pandora FMS

Página en construcción, disculpe la molestia.

Creación de aplicación y obtención de identificadores

Primero se debe iniciar sesión en el portal de https://portal.azure.com/ y buscar Azure Active Directory. Se recomienda implementar doble autenticación en Azure para aumentar la seguridad en el acceso.

Se hace clic en Registro de aplicación → Nuevo registro.

Se rellena la información según la necesidad que se tenga. En este ejemplo se utiliza MSFT (inquilino único).

Una vez creada la aplicación se podrá localizar tanto el `tenantId` (identificador de aplicación de cliente) como el `clientID` (identificador de directorio de inquilino) en la información general de la aplicación.

Para obtener el valor del secreto se debe ir a Certificados y secretos → Nuevo secreto de cliente.

Se deben seguir las indicaciones mostradas y crear el secreto.

En el siguiente paso se debemos copiar el valor del secreto, esto debe hacerse inmediatamente al crear el mismo ya que el valor quedará oculto y no se volverá a mostrar.

Si se actualiza la página el único ID que se conserva es el marcado en la imagen y que el 'Valor' solo se mostrará una parte y sin poder visualizar el resto.

Permisos de API

Ahora se deben agregar los permisos necesarios a la aplicación. Para ello se va a Permisos de API → Agregar permiso → Microsoft Graphy y agregar los siguientes permisos:

Por último se debe ir a Exponer una API → Agregar un ámbito para poder agregar dicho ámbito a la aplicación recién creada en la sección anterior. En caso de que ponga que no se tiene una dirección URI agregada, se deberá hacer clic en siguiente y luego configurar el ámbito de una forma similar a la indicada a continuación:

Una vez realizados todos los pasos y con la información recabada, se puede registrar la aplicación en Integria IMS.

Doble autenticación en Azure

Más que una doble autenticación, en Microsoft Azure® se utiliza una autenticación multifactorial, *Azure AD Multi-Factor Authentication* (MFA) que incluye SMS con código de verificación, una aplicación como Microsoft Authenticator app o Google Authenticator, un escaneo de huella digital, etcétera.

A continuación se muestra un resumen muy simplificado del proceso, para todos los detalles consulte "Tutorial: Secure user sign-in events with Azure AD Multi-Factor Authentication".

- Se recomienda utilizar una Política de acceso condicional la cual puede ser asignada a usuarios, grupos y aplicaciones y que será la encargada de responder a las peticiones de inicio de sesión.
- Es por tanto necesario que se tengan usuarios no administradores ya creados y asignados a grupos de trabajo creados para tal efecto. Dicho trabajo escapa del alcance de este tutorial.
- Para crear una Política de acceso condicional inicie sesión en el portal de Azure con los derechos necesarios (*global administrator*).
- En el menú del lado izquierdo vaya a Azure Active Directory → Security.
- Seleccione Conditional Access → New policy → Create new policy.
- Coloque un nombre, por ejemplo `MFA Pilot`.
- En Assignments seleccione Users or workload identities.
- En What does this policy apply to? verifique que usuarios y grupos esté seleccionado.
- Ahora en Include escoja Select users and groups y marque Users and groups.
- Ya que estará vacío, se abrirá automaticamente un cuadro de diálogo. Seleccione su grupo Azure AD, pongamos por caso que se haya creado con el nombre `MFA-Test-Group`, seleccione dicho grupo.
- Ahora se deben asignar las aplicaciones que utilizarán dicha Política de acceso condicional. El

ejemplo a continuación asume que será aplicado solamente al portal Azure.

1. En Cloud apps or actions vaya a Select what this policy applies to y verifique que Cloud apps se encuentre seleccionado.
2. En Include escoja Select apps.
3. Examine la lista y busque Microsoft Azure Management y márquelo como seleccionado.
4. Ahora se deben configurar los controles de acceso de la MFA, vaya a Access controls → Grant → Grant access.
5. Seleccione Require multi-factor authentication márquelo como seleccionado y pulse l botón Select.

Ahora solamente queda activar la política, vaya a Enable policy seleccione el valor On y pulse el botón Create.

Desde este momento los usuarios y grupos creados que accedan al portal Azure deberán seleccionar el método de la Mobile app en el paso número uno y marcar Use verification code y pulsar el botón Setup para comenzar a configurar la aplicación personal Microsoft Authenticator app o bien Google Authenticator.

Configuración de correo en Integria IMS

Se debe acceder, con los permisos necesarios, al menú Setup → Setup → Email setup y se completan los campos con la información obtenida, por ejemplo:

Consulte la "Configuración avanzada IIMS" para más detalles.

Doble autenticación en IIMS

Se recomienda implementar el segundo factor de autenticación en Integria IMS para aumentar la seguridad en el acceso a las aplicaciones. Consulte "Doble autenticación" para más detalles.

Volver al índice de documentación de Pandora FMS