

Let the good guys in *Yes*

Let us help you with the onerous and complex task of continually monitoring and managing the large numbers of users who access your corporate network and resources each day.

Highlights

- Gain access to skilled resources and best-of-breed technology and monitoring equipment to help ensure only authorised users have access to your corporate network
- Comprehensive discovery, profiling, policy-based placement, and monitoring of endpoint devices on the network
- Enables consistent policies using centralised or distributed deployments
- Comprehensive guest access management – visibility, identification and control
- Can support numerous deployment scenarios from small office to large enterprise environments

Every day users are logging onto your network to access systems and applications. To keep your network and information safe you need to be sure that only authenticated users gain entry and their use is kept within the boundaries you want for them.

Today the problem has compounded because many organisations have a growing number of mobile users – users that want to use their own devices rather than being restricted to a carefully chosen corporate standard. Your Identity and Access Management solution therefore needs to cope with a wide diversity of devices if you are to move ahead confidently with a Bring-Your-Own-Device (BYOD) strategy.

In most businesses there are also guests coming and going, needing secure temporary access during the time they are working with you.

It's a huge task administering, validating and keeping on top of it all. What's more you need to make sure the authentication engines are kept up and running so the access lines are open, letting people get on with their work.

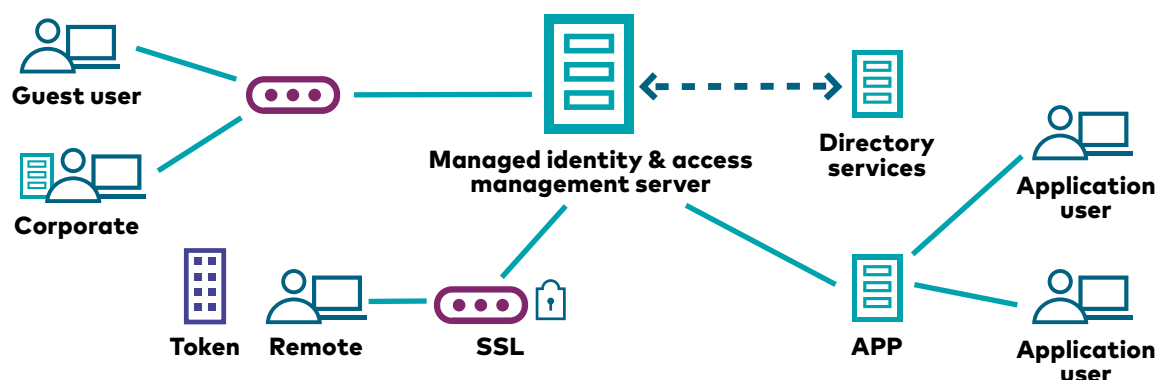
This is where a Managed Identity and Access Management Service from Optus comes in. We can help you to select a solution that meets the specific security needs of your organisation and be there staying vigilant to help keep things running smoothly.

How it works

An Optus Managed Identity and Access Management policy server is deployed in your network environment. The policies configured in that server are used to allow, reject or restrict the user's access.

This server is usually integrated with your directory services where user administration occurs. Identity and Access Management systems can also have self-service capability to give end-users access to a management portal to perform basic administration tasks such as updating their user profile and changing their token pin.

The Identity and Access Management system is transparent and seamless to your end-users.



Identity and access management functions

Depending on the solution and services chosen the following functions can be provided:

Authentication

The solution is designed to authenticate users based on the policies in the Managed Identity and Access Management server. We can assist you in establishing robust and consistent authentication policies including centralised and distributed deployments.

Dual factor authentication

You may choose to use dual factor authentication as an additional level of security. This is often in the form of a hardware token to generate an additional pass code that the user must supply to gain access permission. Other options include software authenticators, on-demand authenticators that send an SMS to the user access credentials and security questions.

Directory integration

Tight Integration with your corporate directory servers, such as Active Directory and LDAP, enables you to have more granular role-based access control policies.

End user self service

With this option your end-users are provided with access to a self-service portal to undertake basic administration tasks, such as:

- Updating user profiles
- Changing their token PIN
- Token test and synchronisation
- Updating security questions

BYOD

Our BYOD services implementation provides a solution capable of working with a diversity of mobile devices so you can allow users to bring their own devices into your wired or wireless network.

Guest services

To enable guests to safely access to your network, we can provide user access and policy enforcement for guest users including custom portal creation for sponsors and guests, sponsor management, guest user creation and time-based access policies with optional posture assessment.

Endpoint services

A range of endpoint services are available including profiling services to assist in identifying, locating and determining the capabilities of all endpoints on the wired or wireless network and posture services to provide assessment and policy enforcement for endpoints.

High availability

Overall fault tolerance of your solution can be increased by using a resilient configuration that supports failover in the event of a critical failure.

Security Event Management

Security Event Management correlates security data from the multiple security devices and systems in your network, including Identity and Access Management solutions. This enables more comprehensive security assessment so appropriate remedial action can be taken promptly. Through our Managed Security Event Management Service you can have 24 x 7 event monitoring across your security environment.

Feature availability

Optus works with industry leading vendors to provide best-of-breed technology solutions. The table below shows the service options available.

Standard Features

Single Factor Authentication

Dual- Factor Authentication

SISE Users

Optional Features

High Availability

Directory Integration

End-user Self Service

SISE Authentication

Profiling

Guest Services

Posture

BYOD

Endpoint Protection Service

Security Event Management

Log retention and storage

Let Optus manage your security

We want to help to reduce your exposure to security threats and incidents. Our aim is to assist you with protecting your valuable intellectual property and complying with legislative requirements.

We can help you to assess, design, implement and manage your security environment so you can move ahead with confidence knowing the confidentiality, integrity, availability and protection of your critical business data is in hand.

Through our managed services you have access to our experienced and skilled team to supplement your own resources.

Whether is it just one aspect of security such as Identity and Access Management or our whole suite of integrated security solutions, choose the peace of mind offered by Optus.