RSA SecurID® Access

Secure access from ground to cloud

Partner sales and marketing
license upgrade guide

Explore ›

Authentication challenges for enterprises

Reselling Tech Data's Recon Managed Identity Services

Enterprise and Premium license features

Use cases

Sales and marketing resources

Download ebook

SecurID® Access

ccess from ground to cloud

es and marketing

grade guide

Authentication challenges for growing and large enterprises

Explore the common authentication challenges facing enterprises managing authentication over a WAN.

Read more >

Authentication challenges for growing and large enterprises

Optimising performance across Wide Area Networks

Ensuring resilience and zero authentication downtime

Ensuring authentication is as unobtrusive as possible

Achieving secure and convenient access

Your largest customers operate from multiple offices over wide geographical areas, and need to successfully be able to authenticate large workforces consisting of thousands of employees.

This high scale of users and increased distance to the primary datacentre across a WAN can result in challenges relating to effective administration, authentication latency and overall workforce productivity.

Authentication challenges for growing and large enterprises

| Optimising performance across Wide Area Networks | Ensuring resilience and zero authentication downtime | Ensuring authentication is as unobtrusive as possible | Achieving secure and convenient access |

Without replica instances of your authentication infrastructure, it can be challenging for enterprises to guarantee that their authentication requirements are online in the case of emergency or routine maintenance.

Authentication challenges for growing and large enterprises

Optimising performance across Wide Area Networks

Ensuring resilience and zero authentication downtime

Ensuring authentication is as unobtrusive as possible

Achieving secure and convenient access

Authentication requires an active input from the user in order to verify they are who they say they are.

Without intelligent measures in place, this can result in lower productivity and avoidable frustration from the user.

Authentication challenges for growing and large enterprises

Optimising performance across Wide Area Networks

Ensuring resilience and zero authentication downtime

Ensuring authentication is as unobtrusive as possible

Achieving secure and convenient access

Identity authentication requires specialist IT expertise, access to the right technologies and an understanding of today's rapidly-evolving threats and trends. This can put already stretched IT resources under strain and lessen the ability to focus on other critical IT projects.

To help our partners solve this problem in an effective and profitable way, Tech Data offers a fully managed service that can be resold by channel partners.

Discover Tech Data's Recon Managed Identity Service ›

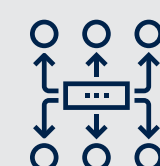# Reselling Tech Data's Recon Managed Identity Services

Utilise Tech Data's security expertise and offer your customers a fully managed security service.

Read more ›

CONNECTION
ANALYSIS
DATA
SEARCHING
VERIFICATION
CODING
SENDING

Add managed identity into your services portfolio with Tech Data

Features

Tech Data's Managed Identity service Recon is a cloud based service that allows Tech Data business partners to provide their customers with access to the expertise and support of skilled and certified RSA SecurID engineers.
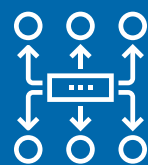
This service allows security partners to develop their security services portfolio and provide a managed identity service without the need to invest upfront in training and infrastructure.

Download Recon brochure ❯

23.1%

Between 2014 to 2020, the number of connected things will grow at an annual compound rate of 23.1%

Add managed identity into your services portfolio with Tech Data

Features

Recon Managed Identity offers flexible levels of support to match the individual requirements of your customers.

The service includes 24 x 7 x 365 support, updates, user management and reporting, all managed by Tech Data but white labeled by the partner. Tech Data engineers can deliver everything for partners from the beginning to the end and partners don't have to worry about anything.

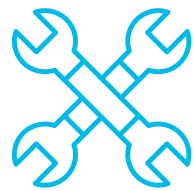**Download Recon brochure** ›

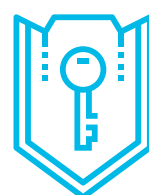## RECON™ Managed Identity Service

Setup

Help desk

Trouble shooting

Software support and updates

User and token management

Quarterly reporting

RSA SecurID® Enterprise and Premium license features

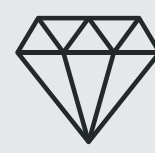Discover how your enterprise customers benefit from upgrading their licenses to Enterprise or Premium.

Read more

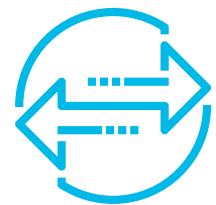License Overview | Enterprise Benefits | Premium Benefits | Comparison Matrix

Introducing RSA SecurID® Enterprise and Premium Licenses

For large scale enterprises or for those that are anticipating growth, opening new offices or acquiring businesses, RSA and Tech Data offer Enterprise and Premium SecurID Access licenses.

Why upgrade?

Improved scalability

Configuration and productivity features

Enhanced performance

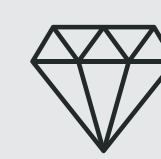Increased resilience

Lower overall TCO!

License Overview

Enterprise Benefits

Premium Benefits

Comparison Matrix

Improve performance, resilience and productivity across large networks with RSA SecurID® Access Enterprise

Upgrading to the SecurID Access Enterprise license provides your customers with access to up to 15 replica instances, allowing your customers to improve performance and resilience across large-scale or multi-site deployments.

Enterprise customers also gain access to Authentication Manager Bulk Administrator (AMBA), which greatly reduces the time to create new, amend or delete users and authentication requirements.

✓ Improve performance, resilience and productivity across large WANs by deploying up to 15 Authentication Manager (AM) replica instances

✓ Reduce workloads with Authentication Manager Bulk Administration (AMBA) capabilities

✓ Lower TCO through greatly reduced administration time and higher resilience

Enterprise cloud customers receive additional access Policy Engine Attributes:

✓ IP Address

✓ Authentication Type

✓ Authentication Source

✓ Country

✓ Known Browser

✓ Trusted Location

✓ Trusted Network

✓ User Agent

License Overview

Enterprise Benefits

Premium Benefits

Comparison Matrix

Create the perfect balance of security and productivity with SecurID® Access Premium licenses

The highest tier of SecurID license - Premium - offers everything available in Enterprise, and additionally enhances the risk engine by adding Identity Confidence capabilities.

This feature improves user productivity and overall security by utilising machine learning and confidence scores across user behavior, device and location to prompt authentication when necessary.

As well as improving the experience for the user, this feature also allows you to determine the effectiveness of your security policies and utilise identity context parameters across individual use cases.

✓ Develop a dynamic risk-based identity assurance strategy, based on a range of contextual, risk and advanced authorization policies, further reducing the risk of friction from users.

✓ Greater ability to map user-level or group-level identity risk factors to your organizational policies, improving security posture.

| Editions	Base	Enterprise	Premium
1. What edition you need based on what you want to protect?	VPN & traditional on-prem agents	VPN & traditional on-prem agents	VPN & traditional on-prem agents
		SaaS, Cloud and SSO	SaaS, Cloud and SSO
	SaaS, Cloud and SSO	**Enterprise Scalability Multiple replicas, AMBA**	**Enterprise Scalability Multiple replicas, AMBA**
			Risk-Based Analytics Contact, risk and adv. auth policies
2. How do you want to protect it?	**Mobile MFA** OTP, push, device biometrics	**Mobile MFA** OTP, push, device biometrics, FIDO	**Mobile MFA** OTP, push, device biometrics, FIDO
	RSA SecurID® Tokens Hardware and Software	**RSA SecurID® Tokens** Hardware and Software	**RSA SecurID® Tokens** Hardware and Software
3. How do you want to deploy and pay for it?	Perpetual or Subscription	Perpetual or Subscription	Subscription only
	Hybrid or All Cloud[1]	Hybrid or All Cloud[1]	Hybrid or All Cloud[1]

1 - Hybrid deployment required to use RSA SecurID tokens, traditional RSA SecurID agents, and/or the SSO agent

Enterprise and Premium use cases

Utilise these use cases and questions to identify opportunities with your customer

Discover use cases ›
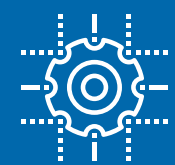
Local replica instances
Disaster Recovery
Manage spikes in demand
Quickly onboard large numbers
Improve security posture

Improve performance and reduce network latency by providing local replica instances

Challenge

Authentication performance can suffer when high numbers of users must log on from geographically remote offices across a WAN.

Potential use cases

Organisation is utilising base licenses and suffering from general latency/performance issues at secondary sites

Organisation opens new secondary office or site

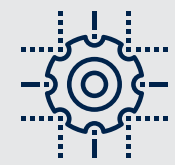New sites acquired as part of corporate merger or buyout

Solution

✓ With RSA SecurID Access Enterprise and Premium, your customers can improve performance and reliability by locating replica instances physically closer to the users who require authentication.

✓ An organization with a headquarters and multiple remote sites can reduce the distance-based latency and improve authentication performance by placing a SecurID Access replica instance at each remote site.

Conversation starters

1. Are your users facing a few seconds of delay when being faced with authentication?

2. Do you have offices across multiple regions/countries?

3. Do you have any upcoming plans to onboard a high number of staff in a new location?
(e.g. new office site or merger)
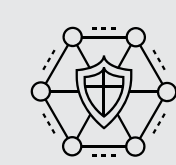
Local replica instances

Disaster Recovery

Manage spikes in demand

Quickly onboard large numbers

Improve security posture

Disaster recovery and maintenance

Challenge

Without replica instances, disaster recovery is limited. This could result in otherwise avoidable authentication downtime due to maintenance, power cuts, network outages or fire and flood damage.

Potential use cases

RSA SecurID Access Enterprise and Premium allows your customers to avoid suspending authentication by creating up to 14 replica instances that can be promoted to the primary instance as disaster recovery, if the primary instance is unresponsive, or as a temporary failover for maintenance.

By making sure deployments have sufficient instances installed to provide authentication while repairs are made, authentication can continue to take place while the primary instance is repaired or if a network connection between sites fails.

Solution

✓ Satellite office loses connection with HQ or main datacentre without causing local authentication downtime

✓ Maintenance work required on primary instance doesn't impact authentication capabilities

✓ Replica instance fails over following fire, flood or blackout at primary or secondary site

✓ Replica instances can support a sudden increase in the number of remote authentications when Business Continuity licenses are activated, leading to an unprecedented surge of users authenticating remotely, e.g. as seen with Covid-19.

Conversation starters

1. Have you had any instances of unplanned authentication downtime in the recent past?

2. Do you have any backup capabilities for your authentication estate?

3. What do you do to keep protecting users and data during planned downtime?
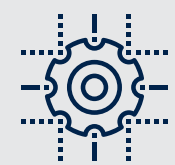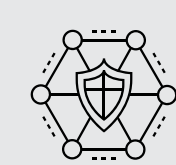
Local replica instances

Disaster Recovery

Manage spikes in demand

Quickly onboard large numbers

Improve security posture

Scaling and managing high levels of authentication

Challenge

As your customer's business continues to grow, they must consider the size of their current user population and the anticipated size of their future user population to prepare for the increased demand for authentication.

Potential use cases

Prepare for spikes in demand, e.g. at the start of the day and after lunch, without reduced impact on performance.

Improve performance at remote sites with significant user populations.

Utilise bulk administrator (AMBA) to quickly onboard new users and ensure optimum ongoing performance.
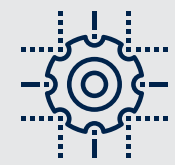
Solution

✓ RSA's SecurID Enterprise and Premium scalability features allow your customer to support growth and temporary peaks in demand.

✓ As your customer's business grows, a multiple replica instance installed on hardware that meets or exceeds the minimum system requirements can help to ensure they have excess capacity to handle increases in demand.
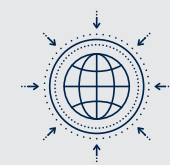
Conversation starters

1. Do you experience latency or performance issues at the start of the day or during spikes of activity?

2. Is adding new users laborious and time-consuming?

3. Do you have any upcoming plans to onboard a high number of staff in a new location? (e.g. new office site or merger)
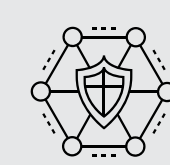
Navigation tabs

- Local replica instances
- Disaster Recovery
- Manage spikes in demand
- **Quickly onboard large numbers**
- Improve security posture

Reduce manual admin with bulk administrator (AMBA)

Challenge

Manual provisioning of new users, removal of old users and changes to policies and groups is a time-consuming and laborious task without automation capabilities.

Potential use cases

Quickly onboard and manage new users:

Onboard new departments, or even offices.

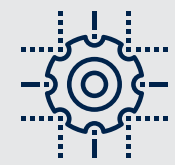Quickly roll out SecurID across entire enterprise.

Scale from pilot quickly and efficiently.

Solution

✓ With Enterprise and Premium, your customers gain access to Authentication Manager Bulk Administration (AMBA). This tool greatly reduces the time required for administrators to manage users, groups, tokens and actions.

✓ This greatly lowers operational costs and prevents administrators from having to manually add or amend users and distribute tokens one by one, allowing IT resources to be utilised on more strategic projects, upgrades and optimisation.

Conversation starters

1. How much time are your administrators spending managing users and groups?

2. Are you in control of your expired users and old groups?

3. Do you ever need to onboard or remove large numbers of users at one time?

| Local replica instances | Disaster Recovery | Manage spikes in demand | Quickly onboard large numbers | Improve security posture |

Improve overall security posture and improve productivity with Identity Confidence

Challenge

Authentication every single time an application, network or device is accessed could reduce in a loss of productivity, especially if it takes a while to authenticate each time.

Potential use cases

Reduce friction with users by reducing requirement to authenticate.

Instantly identify suspicious out-of-ordinary behavior.

Improve security posture and make informed identity context driven risk management decisions.

Solution

✓ With Premium, your customers can leverage Risk Based Identity Confidence to authenticate based on levels of confidence accrued by reviewing user behaviour, location and device.

✓ This reduces friction for users by silently reviewing in the background, only requesting authentication when the access confidence score is lower than required. This also allows for an active review of individual use cases and user sets to increase security confidence for key applications or access requirements such as CRM.

Conversation starters

1. Are your users authenticating at every login?

2. Do you experience resistance around authentication from users?

3. Can you determine the effectiveness of your security policies?

TechData

Sales and marketing resources

Utilise these pre-packaged co-brandable sales and marketing resources to help you create new opportunities for your business
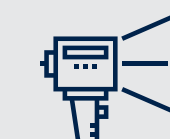
Read more ❯

Tech Data
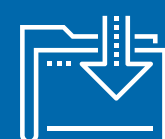
RSA

Download your sales and marketing resources

On the below links you'll find all the resources you need to quick-start your own marketing campaign. View additional tips and ideas across the other 3 tabs in this section.

Brochure

Provide insight and offer value with this solution guide

DOWNLOAD

Marketing Emails

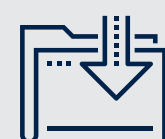Raise awareness and generate marketing leads with these email communications

DOWNLOAD

Social Media Kit

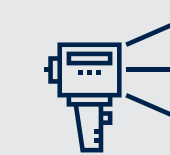Raise awareness with these LinkedIn and Twitter posts

DOWNLOAD

TechData

RSA

Asset Downloads

Brochure
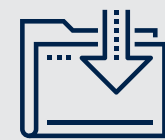
Email

Social Media

Support your sales teams with this brochure

Co-brand this pre-built brochure to quickly provide your sales teams with a comprehensive RSA SecurID Access brochure.

You can utilise this brochure across multiple sales and marketing channels including:

✓ Emailing after a productive sales call

✓ Adding to your website

✓ Sending as part of a promotional email campaign

✓ Training your sales teams
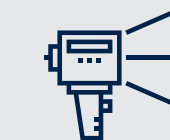
✓ Handing out at events and roadshows

✓ And more!

Brochure

Provide insight and offer value with this solution guide

DOWNLOAD

Asset Downloads

Brochure

Email

Social Media

Email: make sure your database is GDPR compliant!

✓ **It's vital that you maintain good data hygiene**
Ensure your recipients can unsubscribe from future emails and you keep record of your suppressed contacts to comply with data law such as GDPR.

✓ **Make sure you follow up with your prospects!**
Monitoring your email engagement allows you to create warmer opportunities and calling lists for your sales teams to engage with.

✓ **Place the RSA brochure behind a form to build up your database!**
Gating your high-value pieces of content on a landing page behind a form allows you to drive traffic to your website and better qualify your leads.
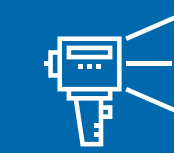
Marketing Emails

Raise awareness and generate marketing leads with these email communications
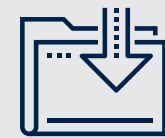
DOWNLOAD

Asset Downloads

Brochure

Email

Social Media

Social Media: LinkedIn is the primary channel for B2B marketing

✓ **46% percent of social media traffic** to B2B company sites originates from LinkedIn*

✓ **79% of B2B Marketers** agree that LinkedIn is an effective source for generating leads*

Social Media Kit

Raise awareness with these LinkedIn and Twitter posts

DOWNLOAD

Top tips

If you haven't already, create a LinkedIn company page. You can then post content directly to LinkedIn and build up your audience.

Encouraging your colleagues to post on LinkedIn is a great way to show thought leadership and greatly improve reach.

*Source: LinkedIn

For more information contact us at xxxx@techdata.com

Built with Prism Present