# Alberta Health Services

# Remote Access & RSA SecurID Tokens
# Fact Sheet

## Who is this fact sheet meant for?

This fact sheet is meant for anyone needing general information about remote access provided by RSA SecurID Tokens.

If you have suggestions for this fact sheet, contact AHSIdentityServices@ahs.ca

## Need to request or modify an RSA SecurID token?

CLICK here for the AHS IAM Remote User Network Access (RUNA) User Guide. Browse the "Topics in this User Guide".

## Need to know how to set-up and use your RSA SecurID token?

CLICK here for the AHS IAM Remote User Network Access (RUNA) User Guide. Browse the "Setting up your RSA SecurID Token" section of "Topics in the this User Guide".

## Topics in this Fact Sheet

# What is Remote User Network Access (RUNA)?

It is remote access to the AHS Network and / or specific applications offered by AHS. Provided by an RSA SecurID hard token or soft token app on a smart device.

# Is a SecurID token the same as a virtual private network (VPN)?

No. If you work on an AHS computer and need to set up remote access through a Virtual Private Network (VPN), refer to the AHS Remote Access (VPN) Insite page https://insite.albertahealthservices.ca/it/page5585.aspx and follow their access request processes. You may still need remote access using an RSA SecurID token for the AHS Network and some of its systems.

# What is an RSA SecurID Token?

RSA is a company that provides security solutions for digital risk.

An RSA SecurID token can be a hardware device that looks similar to this
or a software application that runs on your smartphone or device with an icon similar to this.

When you are issued either type of SecurID token you will be required to create a 4-digit personal identification number (PIN).  The token generates a number that changes every 60 seconds.  Use your PIN and the digits displayed at the time of login to authenticate your identity.

# Software Token Prerequisites

The following are the prerequisites for requesting a software token.

## Device must be supported

- Apple (iOS) Devices – iPhone, iPad, or iPod Touch
- Android Devices – this is an operating system across many manufacturers of different smartphones.  Examples:  Samsung, Sony, and Google.

## Technical Specifications

- Each type of smart device also has minimum technical requirements.  Please refer to these when trying to download the RSA soft token app on your device.  Check the Google Play ® app store on Android devices, and the App Store ® on Apple devices.
- Whichever smart device you choose must be able to run the latest version of the RSA Soft Token application.

## User Requirements

- a valid email address that can be accessed from the device
- the ability / access to install the software token application on the device
- an internet connection on the device
- an internet connection on another device to access the activation website
- no organizational / departmental restrictions regarding the use of mobile devices
- appropriate approval process is followed.

# Can I use my SecurID token with any computer application?

No.  SecurID tokens issued by AHS Information Technology are only useful with computer applications that AHS provides access to.

# Can I use my SecurID token with more than one application?

Yes, you can use your SecurID token with more than one application.  You do not need a separate token for each application you use.

Example:  Let's say you already have remote access to Alberta Netcare Portal and you want remote access to Epic (Connect Care).

When you are filling out your AHS IAM request for Epic (Connect Care) access, ask for remote access, indicate you already have a token and provide any requested details.  This is how AHS IAM connects your Epic (Connect Care) access account to your SecurID token account so they work together.  Going forward you can use the same SecurID token to access both Alberta Netcare Portal and Epic (Connect Care) when you are working outside an AHS site.

# What computer systems need a SecurID token?

Clinical applications that AHS provides remote access to require two-factor authentication with a SecurID token.  Example:  Alberta Netcare Portal (ANP).

The AHS Identity & Access Management (AHS IAM) system also requires a SecurID token when accessed outside an AHS facility.

# Who provides SecurID tokens?

AHS IT Access – Remote Access provide both hard and software RSA SecurID tokens.  They provide them to staff of Alberta Health Services, AHS Affiliates, as well as Physicians, Pharmacists, Chiropractors, and many other types of end-users who access AHS clinical and business applications from outside the AHS Network.

Back to top

# Have you forgotten your PIN?

AHS and AHS Affiliate end-users, please call the AHS IT Service Desk 1 877 311 4300.

Community end-users, including end-users of Alberta Netcare Portal, please call the Provincial Service Desk 1-844-542-7876.

Back to top

# Too many failed login attempts?

Three failed login attempts will result in you being locked out for what will feel like the longest 15 minutes ever.  Then you can login again.  We understand, keeping the cat off the keyboard can be a challenge.

Applies to the:  AHS Network, the Identity & Access Management (IAM) system, Citrix login page, the Unified Access Portal (UAP).

Back to top

# Need help with your RSA SecurID Token?

AHS and AHS Affiliate end-users, please call the AHS IT Service Desk 1 877 311 4300.

Community end-users, including end-users of Alberta Netcare Portal, please call the Provincial Service Desk 1-844-542-7876.

Back to top

# Unused tokens are disabled after 180 days (~ 6 months)

If you need your remote access to keep working, make sure you login remotely at least once every 180 days.  This applies to hardware tokens and software tokens on smart phones and computers.

You will NOT be notified about an inactive token.  If you're not sure when you last used your token, and you know you still need it, call the AHS IT Service Desk to ask 1 877 311 4300.  Make a note of it and login regularly.

If your token is disabled due to inactivity, the Service Desk will **not** be able to re-enable it for you.  You will have to submit a Remote User Network Access (RUNA) request in the IAM system https://iam.ahs.ca .  Need help?  Here's a quick link to the RUNA User Guide – it's posted on the IAM Support Page under Learning.

Back to top

# Check your token's expiry date – they don't last forever

- Hardware tokens don't last forever and aren't replaced automatically anymore.
- Software tokens can only be renewed automatically so many times.
- Find out what your token's expiry date is and make a note of it.
- Read on to find out what will happen as the expiry date gets closer.

If your token expires the Service Desk will **not** be able to renew it for you.  You, or your Authorized Approver / Access Administrator, will have to submit a Remote User Network Access (RUNA) request in the IAM system  https://iam.ahs.ca .  Need help?  Here's a quick link to the RUNA User Guide – it's posted on the IAM Support Page under Learning.

## Hardware tokens



You'll find both your hardware token's expiry date and serial number on the back of the device.

**Hard tokens are not replaced automatically anymore.**  As you may have guessed, they are expensive resources, so when your hard token is nearing its expiry date, you'll be sent an email** from "Identity . Management @ Alberta Health Services.ca" with instructions on what to do.  Emails will be sent 90, 60, 45, 30 and 15 days prior to the expiry date.  They will stop as soon as an action is initiated to renew or remove it.  They will resume as the next expiry date approaches.

**That said, IAM does not have email addresses for everyone.  Here's how to check if we do and what to do if we don't.

**IAM has email addresses for most AHS and AHS Affiliate staff.**
You can check your information anytime and make changes as needed.

Go to https://iam.ahs.ca

LOGIN
CLICK Self Service
CLICK View Profile
REVIEW the information and if changes are needed follow the instructions at the top of the screen.

**IAM does not have email addresses for all community end-users.**
If you have access to IAM, follow the instructions above.

If you don't have access to IAM, contact your Authorized Approver / Access Administrator. They will be able to log into IAM on your behalf and add or modify your information using the Network Access Request (NAR) modify process.

Need help?  Here is a link to the NAR User Guide.  It's always available on the IAM Support Page under Learning.

## Software tokens

To find your software token's expiry date, locate its serial number and call the AHS IT Service Desk at 1-877-311-4300.  They can verify your token's expiry date for you.
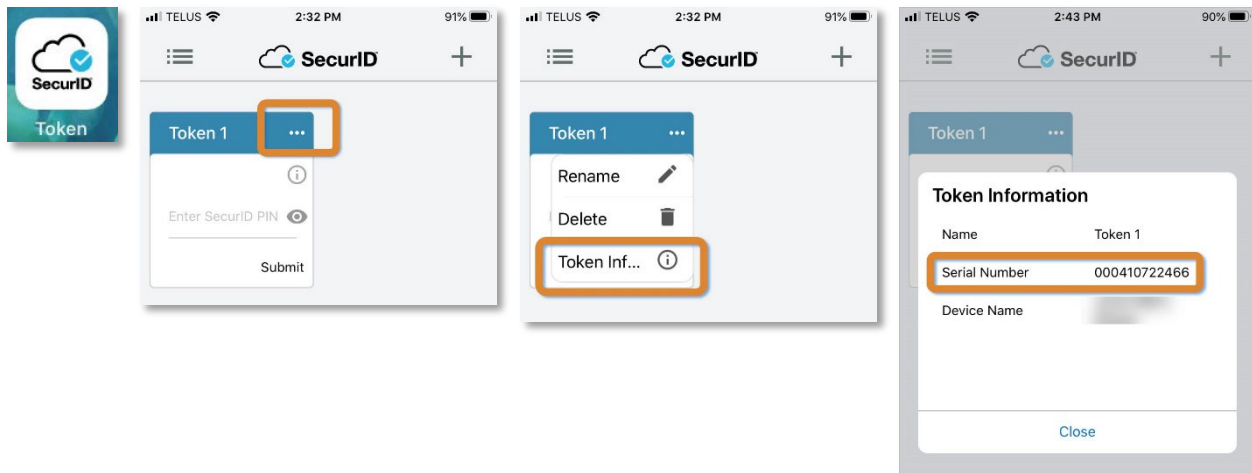
Software tokens **can** be "renewed" automatically a few times with no action needed from you.

If your software token **cannot** be renewed automatically, this is what will happen.

- You'll see notifications in your SecurID app letting you know the expiry date is getting close
- You'll see an on-screen notification in your SecurID app letting you know the expiry date is getting close

You'll be sent email** from "Identity.Management@AlbertaHealthServices.ca" with instructions on what to do to renew your soft token. Emails will be sent 60, 45, 30 and 15 days prior to the expiry date. They will stop as soon as an action is initiated to renew or remove it. They will resume as the next expiry date approaches.

**That said, IAM does not have email addresses for everyone. Here's how to check if we do and what to do if we don't.

**IAM has email addresses for most AHS and AHS Affiliate staff.**
You can check your information anytime and make changes as needed.

Go to https://iam.ahs.ca
LOGIN
CLICK Self Service
CLICK View Profile
REVIEW the information and if changes are needed follow the instructions at the top of the screen.

**IAM does not have email addresses for all community end-users.**

If you have access to IAM, follow the instructions above.

If you don't have access to IAM, contact your Authorized Approver / Access Administrator. They will be able to log into IAM on your behalf and add or modify your information using the Network Access Request (NAR) modify process.

Need help? Here is a link to the NAR User Guide. It's always available on the IAM Support Page under Learning.

Back to top

# Did you see an expiration warning or a notification on your SecurID app?

If your soft token **cannot** be renewed automatically you will see notifications in the RSA SecurID app letting you know the expiry date is getting close. You'll also see an on-screen message that looks similar to this.

Follow the instructions under "Software tokens" in the topic just before this one.



Back to top

# My token has expired, what do I do?

You will have to request a new token.

GO TO the Identity & Access Management (IAM) application:  https://iam.ahs.ca

LOGIN with your AHS network Username and Password

CLICK Request or Modify Access

CLICK For Myself

At Remote User Network Access (RUNA) CLICK Request Access / Change Access

REVIEW and UPDATE your information as necessary

    Soft tokens are recommended

IDENTIFY an Authorizing Manager if needed

CLICK Submit Request

LOGOUT of IAM

More detailed instructions and info can be found in the RUNA User Guide.  It is available to you anytime on the AHS IAM Support Page under Learning.

Back to top

# I don't need my token anymore, what do I do?

1.  Allow it to expire if the expiration date is close.

    OR

2.  If the expiration date is not close, mail your hard token back to IT Access Remote Access in a padded or bubble envelope to:

    AHS IT Remote Access
    CN Tower, 16th Floor,
    10004 – 104 Avenue NW
    Edmonton, Alberta T5J 0K1

    OR

3.  Bring your expired token to your local Eco Station.  Only do this if your hard token has expired. A hard token that still has some life in it can be reused – please return it to IT Access Remote Access.  See option 2 above. 😊

    OR

4. You can also, proactively, remove your remote access using the AHS Identity & Access Management (IAM) system using these steps. This will disable your soft token. If it's a hard token, also see the return steps above.

> GO TO the Identity & Access Management (IAM) application: https://iam.ahs.ca
> LOGIN with your AHS network Username and Password
> CLICK Request or Modify Access
> CLICK For Myself
> CLICK Request Access / Change Access at Remote User Network Access (RUNA)
> SELECT Remove
> IDENTIFY an Authorizing Manager if needed
> CLICK Submit Request
> LOGOUT of IAM

More detailed instructions and info can be found in the RUNA User Guide. It is available to you anytime on the AHS IAM Support Page under Learning.

Back to top

# How do I get a SecurID token?

CLICK here for the AHS IAM Remote User Network Access (RUNA) User Guide. Browse the "Topics in this User Guide".

Back to top

# How do I use my SecurID token?

CLICK here for the AHS IAM Remote User Network Access (RUNA) User Guide. Browse the "Topics in this User Guide".

Back to top

# How to log into AHS IAM Remotely

CLICK here for the AHS IAM Remote User Network Access (RUNA) User Guide. Browse the "Topics in this User Guide".

Back to top

# Additional Resources

CLICK here to launch the AHS IAM Remote User Network Access (RUNA) User Guide
      This guide includes RSA Token Setup and PIN set / reset instructions
CLICK here to launch the AHS Remote Access Standard
CLICK here to launch the AHS Strong Authentication Device User Policy

These resources are also posted on the **IAM Support Page** under **Learning**.

<div align="right">

Back to top

</div>

◆　end　◆