

Remote User Network Access (RUNA) and RSA SecurID Token Set Up User Guide

Who is this guide meant for?

This guide is meant for anyone needing to create, modify or remove remote access to the AHS Network and / or specific applications using the AHS Identity & Access Management (IAM) system.

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

Looking for general information about remote access?

CLICK [here](#) for the Remote Access Fact Sheet.

Additional Resources

- CLICK [here](#) to launch the AHS Remote Access Standard
- CLICK [here](#) to launch the AHS Strong Authentication Device User Policy
- CLICK [here](#) to launch the RSA SecurID Tokens Fact Sheet

These resources are also posted on the IAM Support Page under  [Learning](#).

Topics in this User Guide

Who is this guide meant for?	1
Looking for general information about remote access?	1
Additional Resources	1
Prerequisite AHS IAM Security Profile	3
Prerequisite AHS IAM Network Account	3
What is Remote User Network Access (RUNA)?	3
What is an RSA SecurID Token?	3
What are RUNA request workflows used for and not used for?	4
RSA SecurID Tokens 	4
Virtual Private Network (VPN) 	4

Remote Access to Alberta Netcare Portal (ANP) 	4
Request [new] Remote User Network Access (RUNA)	5
Request RUNA for yourself (Myself)	7
Request RUNA for a New User	8
Request RUNA for an Existing User	9
Request RUNA for Multiple Users	10
Complete Access Request Screen	15
 Tool Tips for the Complete Access Request Screen	16
Approve a RUNA Request	19
Modify or Remove Remote Access	21
 Tool Tips for the Complete Access Request Screen	23
Setting up your RSA SecurID Token	25
Hard Token Set Up	25
Soft Token Set Up	25
Step 1 of 4: Install the RSA SecurID App on your Device – Apple or Android	26
Step 2 of 4: import your unique token into the app	26
Setting your PIN	28
Incorrect login attempts	29
Inactive access	30
Tokens expire	30
Have you forgotten your PIN?	30
Log into AHS IAM Remotely	31
Appendix – AHS IAM Terms & Definitions	33

Prerequisite AHS IAM Security Profile

To use AHS IAM, you must have completed your AHS IAM Security Profile. If you have not created your Security Profile you will be prompted to do so when you first log into AHS IAM. If you need help, click [here](#) to launch the AHS IAM Security Profile User Guide. You can also find it posted on the AHS IAM Support Page under  [Learning](#).

Prerequisite AHS IAM Network Account

Before remote access can be provided to an end-user, they must have a current AHS Network UserID / access account. This would have been provided through the e-People onboarding process or the AHS IAM Network Access Request (NAR) process.

What is Remote User Network Access (RUNA)?

Answer: 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.
- Provided by the Virtual Private Network (VPN) tool, Forticlient.

What is an RSA SecurID Token?

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.

If you need to return your hard token, use a bubble envelope and this mailing address:

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

What are RUNA request workflows used for and not used for?

RSA SecurID Tokens

If you need to access the AHS Identity & Access Management (AHS IAM) system or one of the systems listed below from outside an AHS facility, you will need an RSA SecurID token to provide a second form of authentication when you login.

Many of these applications have the RUNA workflow built into their IAM access provisioning workflows. Go there if this applies to your needs. If not, use the IAM RUNA request process.

AH-ACCIS	Client Registry
AH-AID	CPAR
AH-ARP/APP	CRP-Physical Therapy Clinic VPN
AH-BIE	Epic (Connect Care)
AH-DSR	Epic (Connect Care) - TCA
AH-HLINK	HAP
AH-Imm/ARI (IDSM)	I/Request
AH-NMS	MyApps [Citrix]
AH-PCR	Netcare
AH-Sandbox PLB	VAX Application VPN only
Authorized Approver	VPN
AVBS - Vaccine Booking System	WellSkyTM

Virtual Private Network (VPN)

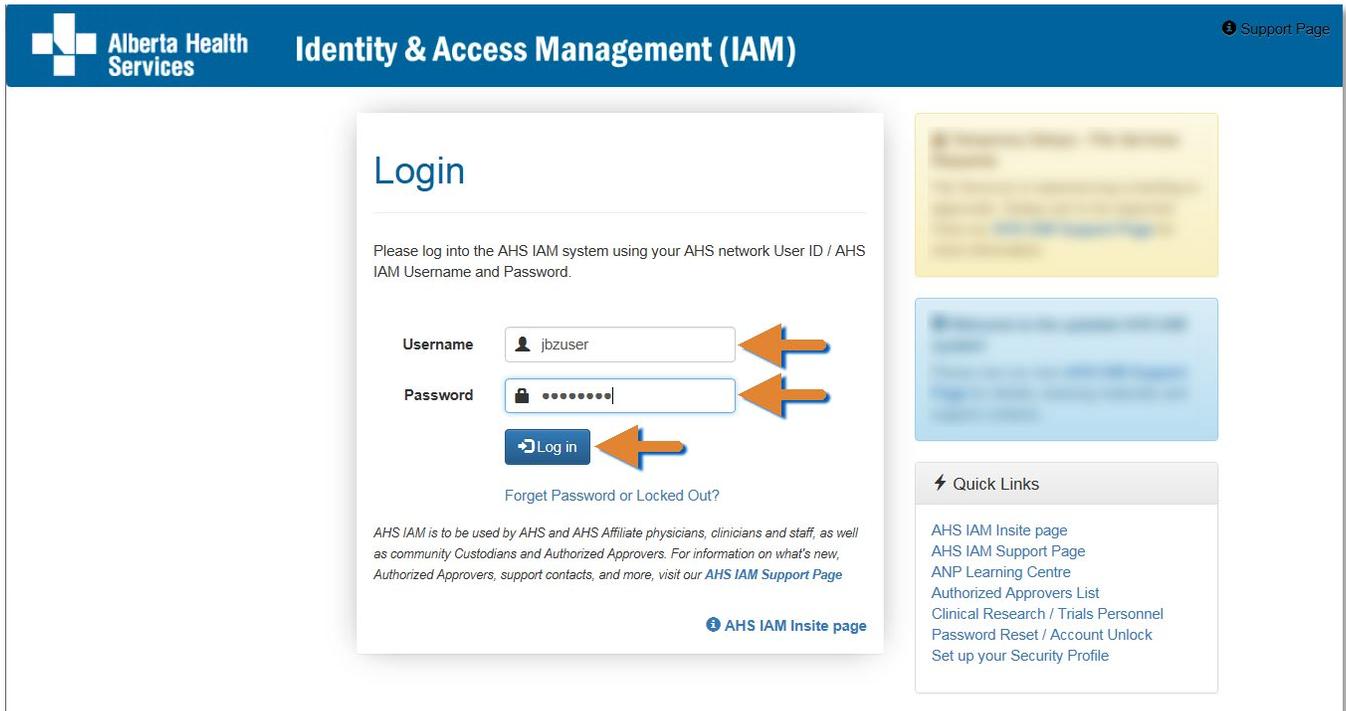
If you need to set up remote access through a Virtual Private Network (VPN), refer to the AHS Remote Access (VPN) Insite page <https://insite.albertahealthservices.ca/it/Page5585.aspx> and follow their access request processes.

Remote Access to Alberta Netcare Portal (ANP)

If you need remote access to Alberta Netcare Portal (ANP), or if you need to modify your existing remote access to ANP, go to the IAM ANP workflows.

Request [new] Remote User Network Access (RUNA)

ENTER the AHS IAM URL into your internet web browser  <https://iam.ahs.ca>
The **AHS IAM Login** screen appears



The screenshot shows the AHS IAM Login page. At the top left is the Alberta Health Services logo and the text "Identity & Access Management (IAM)". At the top right is a "Support Page" link. The main content area is titled "Login" and contains the following elements:

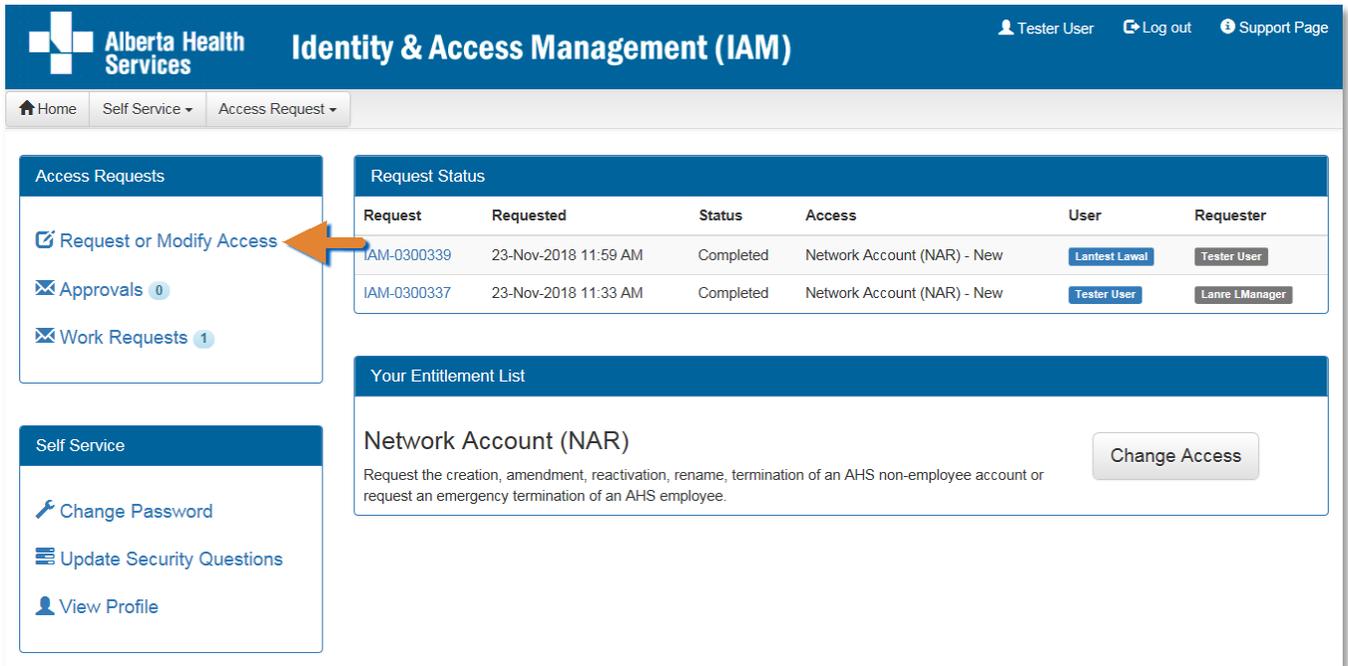
- A message: "Please log into the AHS IAM system using your AHS network User ID / AHS IAM Username and Password."
- A "Username" field with the value "jbzuser".
- A "Password" field with masked characters ".....".
- A "Log in" button.
- A link: "Forgot Password or Locked Out?".
- A footer note: "AHS IAM is to be used by AHS and AHS Affiliate physicians, clinicians and staff, as well as community Custodians and Authorized Approvers. For information on what's new, Authorized Approvers, support contacts, and more, visit our [AHS IAM Support Page](#)".
- A link: "AHS IAM Insite page".
- A "Quick Links" section with the following links:
 - AHS IAM Insite page
 - AHS IAM Support Page
 - ANP Learning Centre
 - Authorized Approvers List
 - Clinical Research / Trials Personnel
 - Password Reset / Account Unlock
 - Set up your Security Profile

Orange arrows in the original image point to the Username field, Password field, and Log in button.

ENTER your **Username** and **Password**

CLICK  **Log in**

The **AHS IAM**  **Home** screen appears



Alberta Health Services Identity & Access Management (IAM)

Tester User Log out Support Page

Home Self Service Access Request

Access Requests

- Request or Modify Access
- Approvals 0
- Work Requests 1

Request Status

Request	Requested	Status	Access	User	Requester
IAM-0300339	23-Nov-2018 11:59 AM	Completed	Network Account (NAR) - New	Lantest Lawal	Tester User
IAM-0300337	23-Nov-2018 11:33 AM	Completed	Network Account (NAR) - New	Tester User	Lanre LManager

Self Service

- Change Password
- Update Security Questions
- View Profile

Your Entitlement List

Network Account (NAR)

Request the creation, amendment, reactivation, rename, termination of an AHS non-employee account or request an emergency termination of an AHS employee.

Change Access

CLICK [Request](#) or [Modify Access](#)

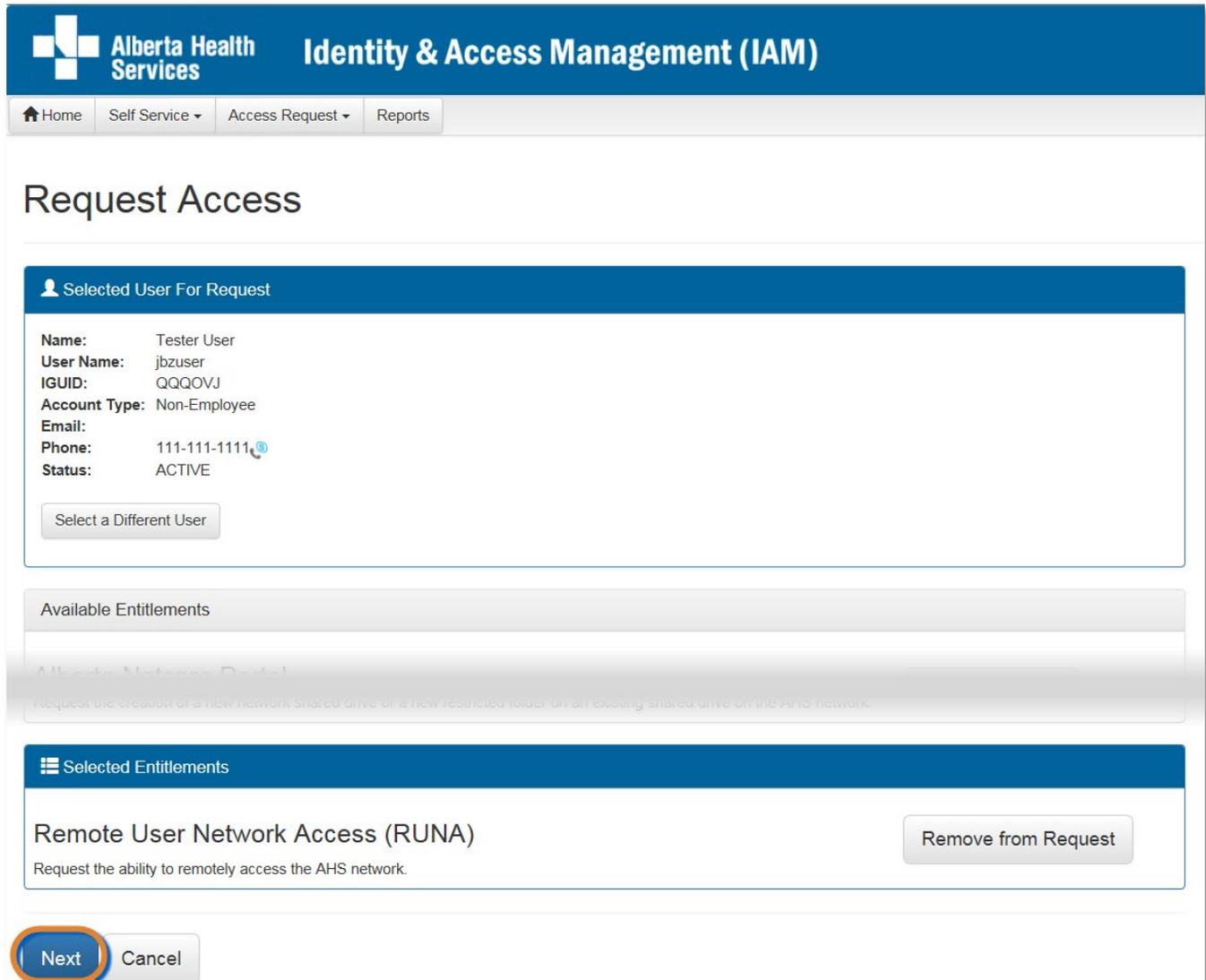
The **Request Access** screen appears

You can create a request for yourself (Myself), an Existing User, Multiple Users, or a New User.

Request RUNA for yourself (Myself)

Click  [Myself](#)

The screen refreshes with your details displayed in the [Selected User for Request](#) pane



The screenshot shows the 'Request Access' page in the IAM system. At the top, there is a navigation bar with 'Home', 'Self Service', 'Access Request', and 'Reports'. The main heading is 'Request Access'. Below this, there is a section titled 'Selected User For Request' with the following details: Name: Tester User, User Name: jbzuser, IGUID: QQQOVJ, Account Type: Non-Employee, Email: (blank), Phone: 111-111-1111, Status: ACTIVE. A 'Select a Different User' button is present. Below this is the 'Available Entitlements' section, which is currently empty. The 'Selected Entitlements' section shows 'Remote User Network Access (RUNA)' with a description 'Request the ability to remotely access the AHS network.' and a 'Remove from Request' button. At the bottom, there are 'Next' and 'Cancel' buttons, with 'Next' highlighted by a red circle.

Under [Available Entitlements](#), at [Remote User Network Access \(RUNA\)](#), CLICK [Request Access](#)

The screen refreshes with the [Selected Entitlements](#) pane at the top of the screen

CLICK [Next](#)

The **Complete Access Request** screen appears

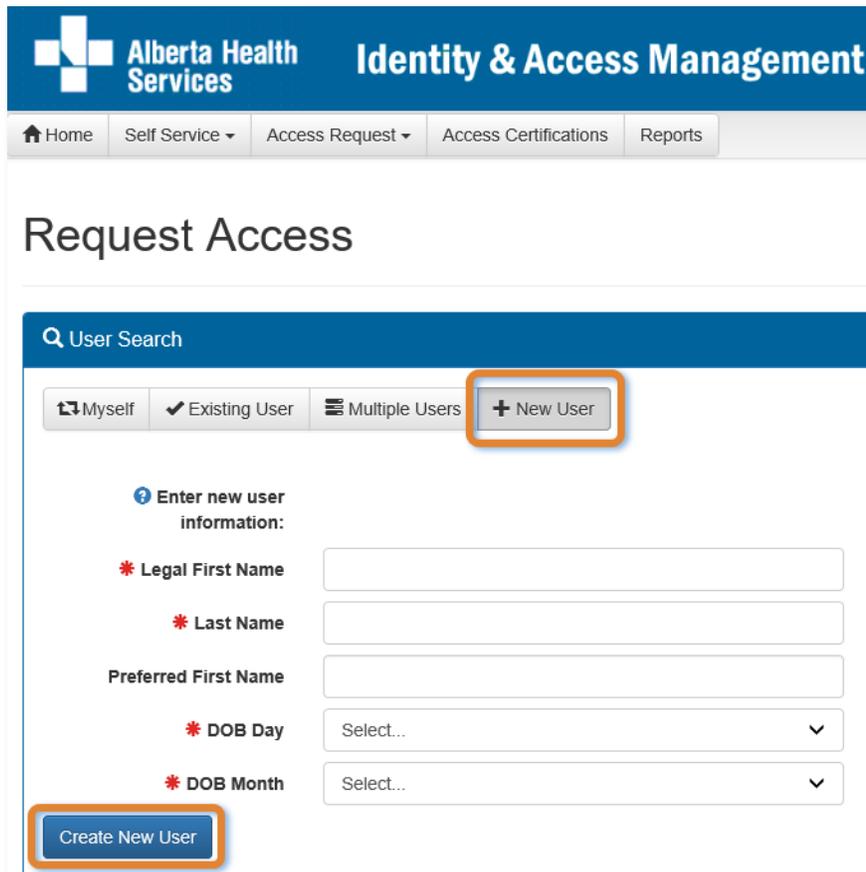
SKIP to [Complete Access Request](#) screen

Request RUNA for a New User

If New User

CLICK **+** [New User](#)

The screen refreshes



ENTER the [Legal First Name](#)

ENTER the [Last Name](#)

ENTER the (Date of Birth) [DOB Month](#) and [DOB Day](#)

CLICK [Create New User](#)

The **Request Access** screen Appears

Under [Available Entitlements](#), at [Remote User Network Access \(RUNA\)](#), CLICK [Request Access](#)

The screen refreshes and the [Selected Entitlements](#) pane appears at the top of the screen

CLICK [Next](#)

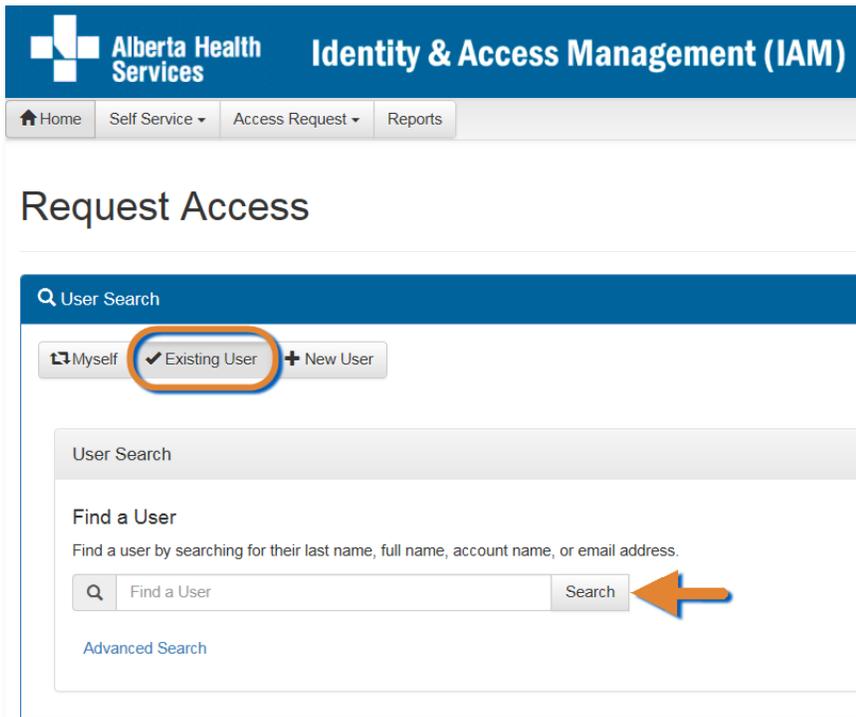
The **Complete Access Request** screen appears

SKIP to [Complete Access Request](#) screen

Request RUNA for an Existing User

If Existing User

CLICK Existing User



The screenshot shows the 'Request Access' page in the AHS IAM system. At the top, there is a navigation bar with 'Home', 'Self Service', 'Access Request', and 'Reports'. Below this is a 'User Search' section with three radio buttons: 'Myself', 'Existing User' (which is selected and circled in orange), and 'New User'. Underneath, there is a 'Find a User' section with a search input field and a 'Search' button, which is pointed to by an orange arrow. There is also a link for 'Advanced Search'.

SEARCH for the existing end-user using the simple or [Advanced Search](#) functions

[User Search Results](#) appear

SELECT the end-user

The **Request Access** screen refreshes with the end-user's details displayed in the [Selected User For Request](#) pane

Under [Available Entitlements](#), at [Remote User Network Access \(RUNA\)](#), CLICK [Request Access](#)

The screen refreshes and the [Selected Entitlements](#) pane appears at the top of the screen

CLICK [Next](#)

The **Complete Access Request** screen appears

CONTINUE to [Complete Access Request](#) screen

Request RUNA for Multiple Users

NOTES:

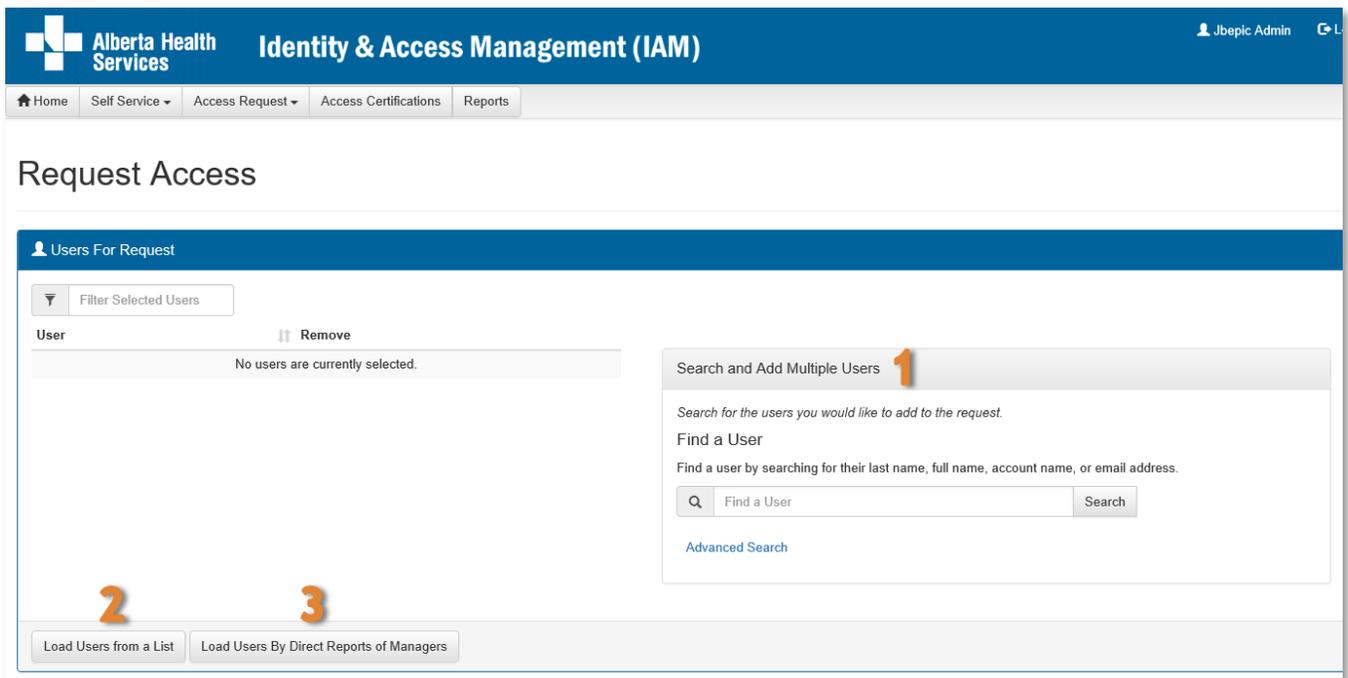
This option is ideal for multiple, existing end-users who have same / similar remote access request needs.

This process will allow you to copy information from one end-user's request to another end-user's request. You will still have the ability modify each request to suit each person's unique situation.

If Multiple Users

CLICK  Existing Users

The **Request Access** screen appears



CREATE your list of end-users using one or a combination of the options below (instructions follow):

Option 1: search for end-users individually → [Search and Add Multiple Users](#)

Option 2: enter a list of users → [Load Users from a List](#)

Option 3: search for end-users by their manager → [Load Users by Direct Reports of Managers](#).

Option 1:

In the [Search and Add Multiple Users](#) pane SEARCH for the end-users individually using the simple or [Advanced Search](#) functions

[User Search Results](#) appear

SELECT the end-users

The selected end-users will appear in a list to the left of the [Search and Add Multiple Users](#) pane. If needed, REMOVE end-users from the list if needed by CLICKING on [Remove icon](#).

Option 2:

CLICK [Load Users from a List](#)

A pop-up window appears



ENTER a list of IGUIDs or User IDS, separated by commas

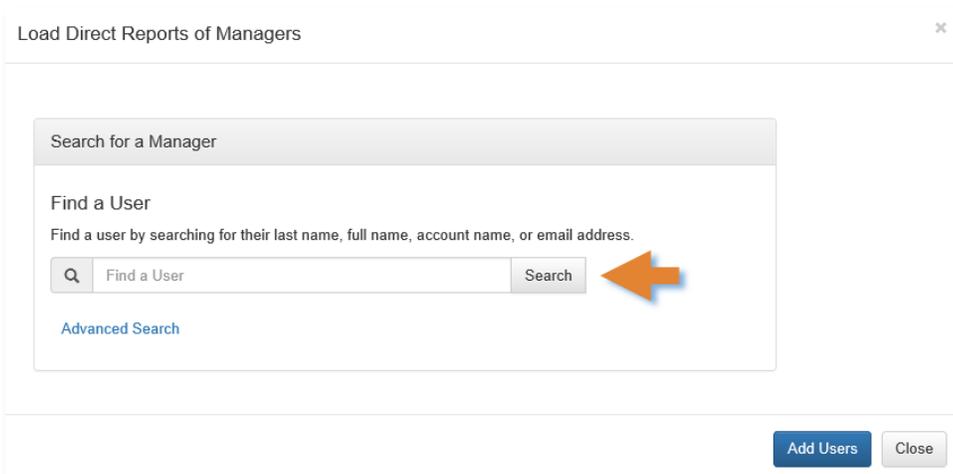
CLICK [Add Users](#)

The selected end-users will appear in a list to the left of the [Search and Add Multiple Users](#) pane. If needed, REMOVE end-users from the list if needed by CLICKING on [Remove icon](#).

Option 3:

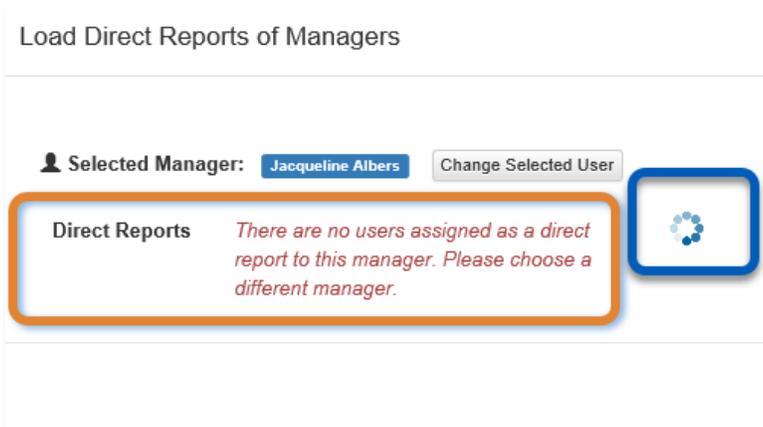
CLICK [Load Users By Direct Reports of Managers](#)

A pop-up window appears

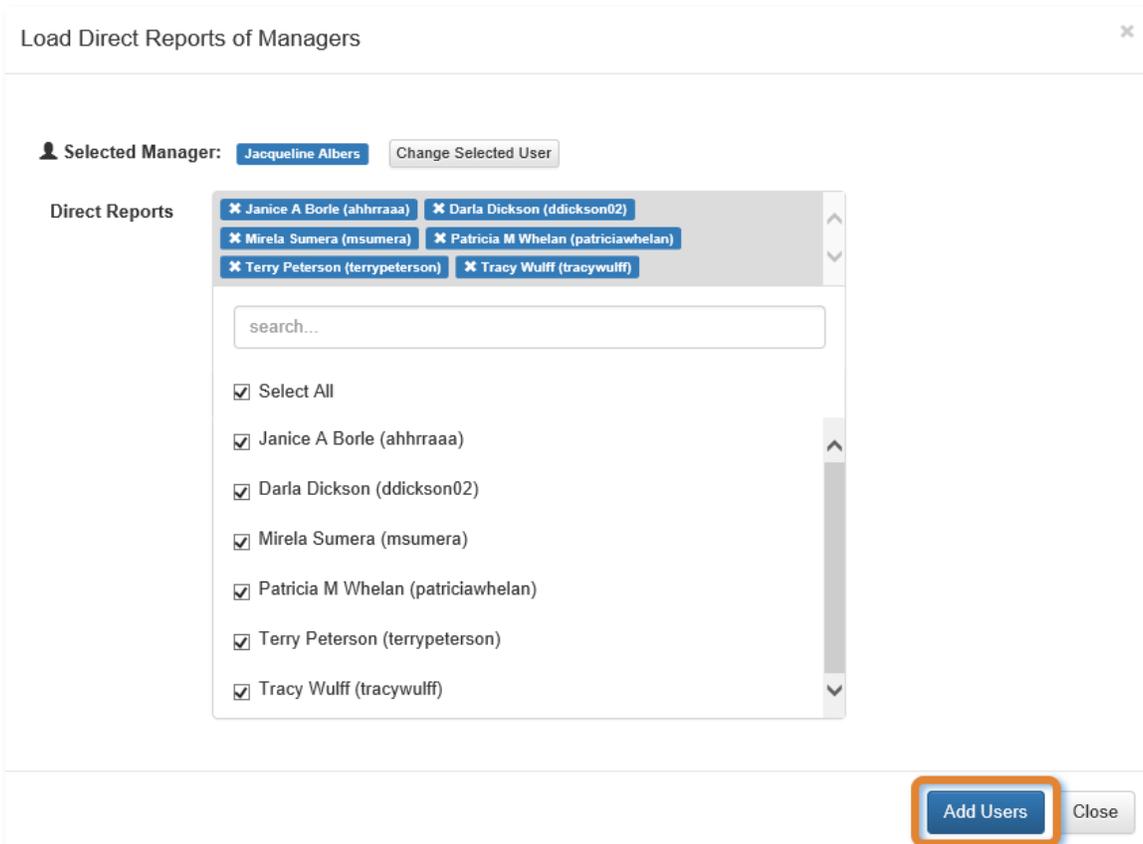


SEARCH for and SELECT the Manager using the simple or [Advanced Search](#) options

An on-screen spinner  indicates IAM is processing the search.
An on-screen message also appears; disregard the on-screen message until the spinner stops.



Search results will appear, but if not, check your search criteria and search again.



UNCHECK end-users you do not want to include in this process
CLICK [Add Users](#)

The **Request Access** screen appears with end-users listed
ADD or REMOVE end-users if needed
The [Available Entitlements](#) pane appears in the lower half of the screen

Under [Available Entitlements](#), at [Remote User Network Access \(RUNA\)](#) CLICK [Request Access](#)
The screen refreshes and the [Selected Entitlements](#) pane appears at the top of the screen

CLICK [Next](#)

The **Request Access for Multiple Users** screen appears with the [Remote User Network Access \(RUNA\)](#) pane displayed for the first end-user in your list. Their status is “draft” in the list of end-users.

You’ll process and submit each end-user’s RUNA request. Those instructions are found at [Complete Access Request](#) screen.

(Optional) CLICK the [Clone Data](#) radio button

This means you will be copying information from the selected end-user’s submitted request into the current draft request. You will still have the ability to modify each request to suit the person’s unique situation. You do not have to use the cloning feature but it can save you time.

IAM processes the records in the order they appear. But you do not have to process end-users in that order; you can complete and submit requests in any order you like.

You can clone data from one request to all the others or select whose data you want the clone to apply to. The end-user’s record highlighted in blue on the list is the access request you’re working in.

REVIEW the access request

ACCEPT or MODIFY the data as needed

CLICK [Submit Request](#)

The selected end-user’s request status is [Pending](#)

The next end-user’s status is [Draft](#) and the [Remote User Network Access \(RUNA\)](#) pane is ready for review.

COMPLETE access requests for each end-user on the list

You must submit each request separately – there is no bulk submit function. This is because IAM must create a unique record for each end-user for their current access requirements and their future role maintenance needs.

Once the last access request has been submitted you will be returned to the **AHS IAM**  **Home** screen

NOTE the [Success The Multiple user request was marked complete](#) highlighted in green at the top of the screen.

NOTE the [Request for Multiple Users](#) pane. If you have saved a multiple user request as a draft it will appear here for you to Resume.

NOTE the [Request Status](#) pane. Each of the end-user's processed in a multiple user request will be listed here for monitoring.

CLICK on the [IAM-#####](#) request number to see an individual access request
The **Request Status Viewer** appears

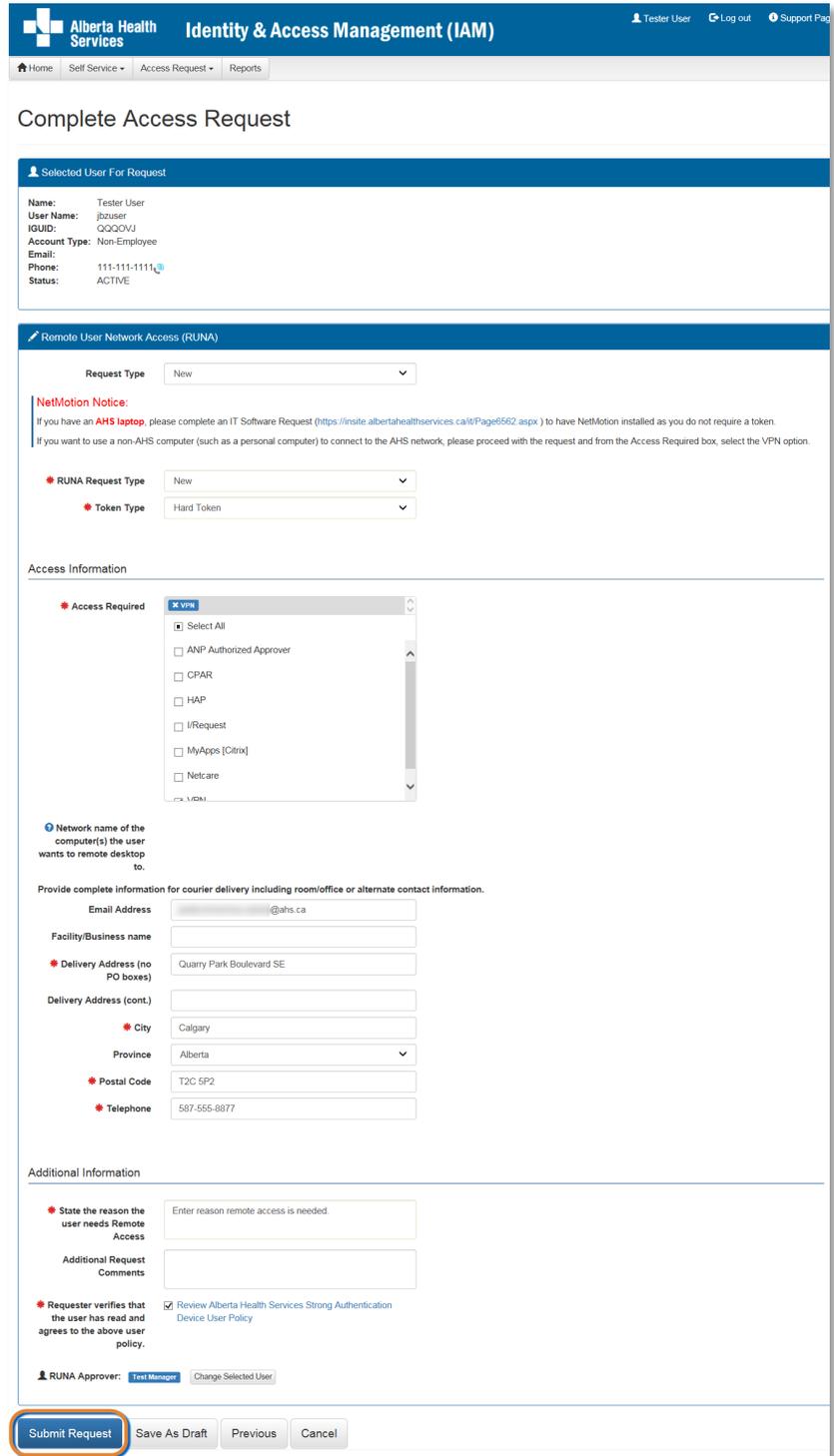
NOTE the request has a status of [Pending](#). Once the end-user has been issued a SecurID token, the request will complete.

Complete Access Request Screen

COMPLETE the  Remote User Network Access (RUNA) pane

READ the on-screen information and field tips

SEE the  Tool Tips on the following page



Alberta Health Services Identity & Access Management (IAM)

Home | Self Service | Access Request | Reports

Complete Access Request

Selected User For Request

Name: Tester User
 User Name: jbzuser
 IGUID: QQQQVJ
 Account Type: Non-Employee
 Email: jbzuser@ahs.ca
 Phone: 111-111-1111
 Status: ACTIVE

Remote User Network Access (RUNA)

Request Type: New

NetMotion Notice:
 If you have an **AHS laptop**, please complete an IT Software Request (<https://insite.albertahealthservices.ca/it/Page6562.aspx>) to have NetMotion installed as you do not require a token.
 If you want to use a non-AHS computer (such as a personal computer) to connect to the AHS network, please proceed with the request and from the Access Required box, select the VPN option.

RUNA Request Type: New
 Token Type: Hard Token

Access Information

Access Required: VPN

- Select All
- ANP Authorized Approver
- CPAR
- HAP
- I/Request
- MyApps [Citrix]
- Netcare
- VPN

Network name of the computer(s) the user wants to remote desktop to.

Provide complete information for courier delivery including room/office or alternate contact information.

Email Address:
 Facility/Business name:
 Delivery Address (no PO boxes):
 Delivery Address (cont.):
 City:
 Province:
 Postal Code:
 Telephone:

Additional Information

State the reason the user needs Remote Access:
 Additional Request Comments:
 Requester verifies that the user has read and agrees to the above user policy: Review Alberta Health Services Strong Authentication Device User Policy

RUNA Approver: [Test Manager](#) | [Change Selected User](#)

Submit Request | Save As Draft | Previous | Cancel

Tool Tips for the Complete Access Request Screen

COMPLETE all mandatory * fields and as many optional fields as possible.

At RUNA Request Type

SELECT one of the following values from the dropdown list.

Existing Token	Select this if the staff member has a token on hand (this is for staff who are moving between community facilities, AHS staff do not need to submit a new RUNA if they move locations, their remote access remains in place for the term of their employment and is available province-wide).
New	Select for a new token.
Transfer	Select if you have an unassigned and unexpired hardware token on hand – check the back of the token for an expiration date.

At Token Type

SELECT **Hard Token** OR **Soft Token**

A Hard Token is a device that looks similar to this



. A Soft Token is a software application that runs on your smartphone or device with an icon similar to this.



At Access Information / Access Required

SELECT all the remote access applications or functions that apply

AH-ACCIS	Client Registry
AH-AID	CPAR
AH-ARP/APP	CRP-Physical Therapy Clinic VPN
AH-BIE	Epic (Connect Care)
AH-DSR	Epic (Connect Care) - TCA
AH-HLINK	HAP
AH-Imm/ARI (IDSM)	I/Request
AH-NMS	MyApps [Citrix]
AH-PCR	Netcare
AH-Sandbox PLB	VAX Application VPN only
Authorized Approver	VPN
AVBS - Vaccine Booking System	WellSkyTM

At Contact Information

ENTER the personal e-mail address that is associated with the device the Soft Token app will be installed on
CONFIRM E-mail

At Additional Information

PROVIDE the reason the end-user needs remote access
CONFIRM the end-user has reviewed the [AHS Strong Authentication Device User Policy](#)

At Select Authorized Approver

If you are an [Authorized Approver](#), you will not have to SELECT an [Approving Manager](#); the request will be automatically approved.

If you are not an [Authorized Approver](#), you will have to SEARCH for and SELECT an [Authorized Approver](#).

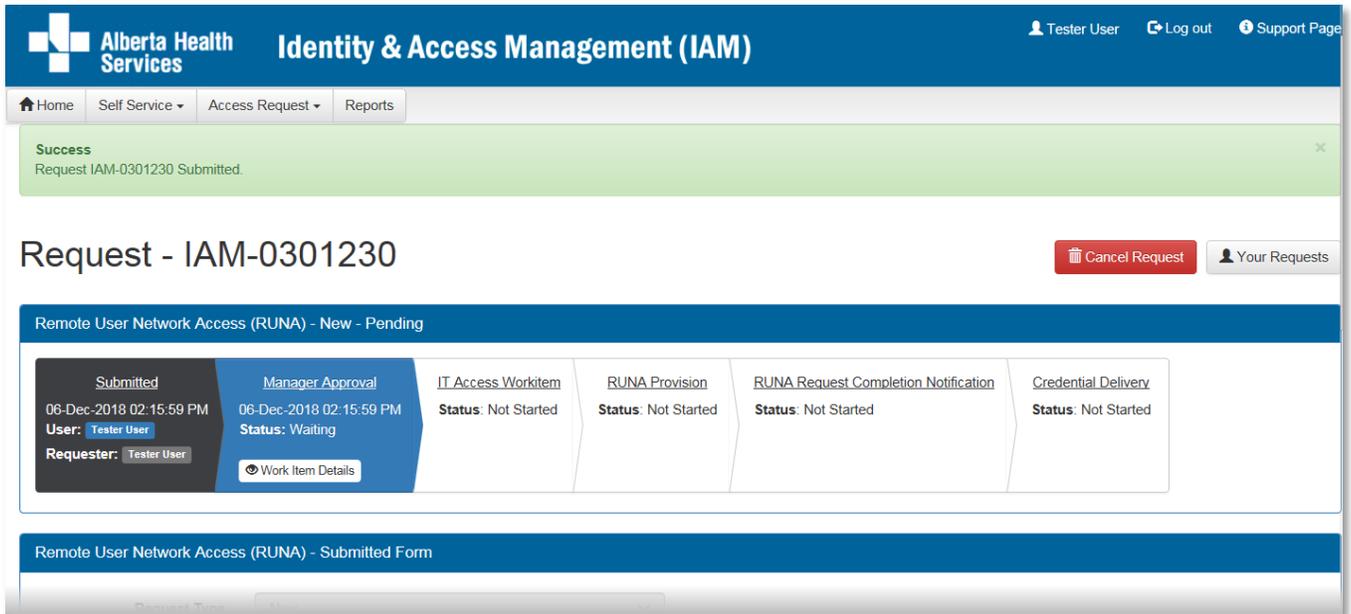
CLICK [Submit Request](#)

The **Request Status Viewer** appears

Note the, “**Success** Request IAM-##### Submitted.” message in the top left corner highlighted in green.

The [Remote User Network Access \(RUNA\) – Submitted Form](#) is displayed for review.

If you are an Authorized Approver the request will be pending at the [IT Access Workitem](#) step.
If you are not an Authorized Approver the request will be [Waiting](#) at the [Manager Approval](#) step – as shown in this example.



The screenshot shows the AHS IAM web interface. At the top, there is a navigation bar with the Alberta Health Services logo and the text "Identity & Access Management (IAM)". On the right side of the navigation bar, there are links for "Tester User", "Log out", and "Support Page". Below the navigation bar, there is a breadcrumb trail: "Home", "Self Service", "Access Request", and "Reports". A green success message banner reads "Success Request IAM-0301230 Submitted." Below this, the main heading is "Request - IAM-0301230" with a "Cancel Request" button and a "Your Requests" link. The main content area is titled "Remote User Network Access (RUNA) - New - Pending" and contains a table with the following columns and data:

Submitted	Manager Approval	IT Access Workitem	RUNA Provision	RUNA Request Completion Notification	Credential Delivery
06-Dec-2018 02:15:59 PM User: Tester User Requester: Tester User	06-Dec-2018 02:15:59 PM Status: Waiting Work Item Details	Status: Not Started	Status: Not Started	Status: Not Started	Status: Not Started

Below the table, there is a section titled "Remote User Network Access (RUNA) - Submitted Form".

CLICK  Home to return to the **AHS IAM**  Home screen
In the [Request Status](#) pane, the request is displayed with a Status of Pending

If you identified an [Authorized Approver](#), they will be notified in two ways:
An email from Identity Management Services will alert them a request requires their approval.
When they login into AHS IAM, the request will be waiting in their [Approvals](#) queue.

Once the request is approved, it will be automatically routed to AHS IT Access Remote Access to provision either the hard or soft token. Hard tokens are mailed to the end-user. Soft tokens are emailed to the end-user with installation instructions.

Complete 

Approve a RUNA Request

This process must be performed by an [Authorized Approver](#)

ENTER the AHS IAM URL into your internet web browser ➡ <https://iam.ahs.ca>

The **AHS IAM Login** screen appears

ENTER your [Username](#) and [Password](#)

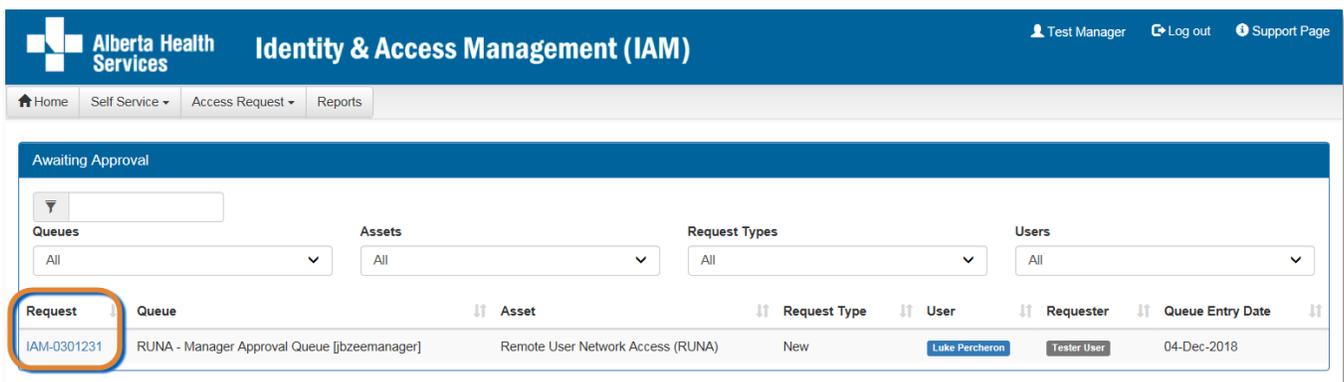
CLICK ➡ [Log in](#)

The **AHS IAM** 🏠 **Home** screen appears



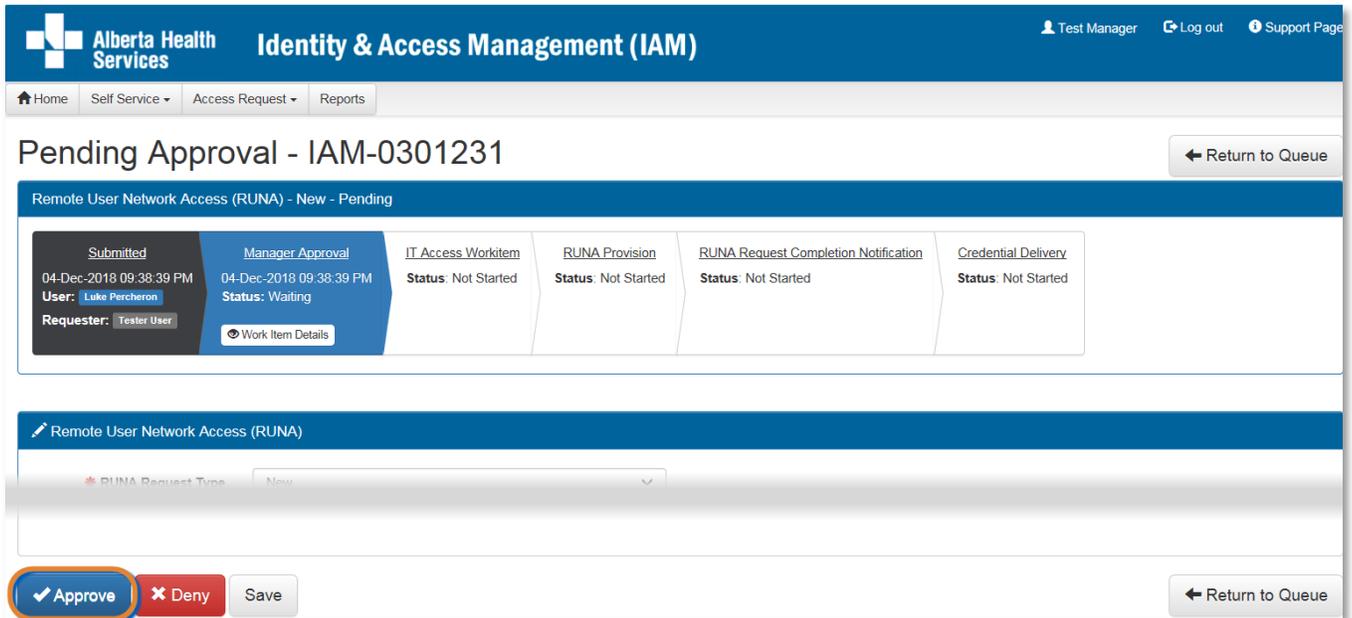
In the [Access Requests](#) pane, CLICK on [Approvals](#)

The **Awaiting Approval** screen appears



CLICK on the IAM request that requires approval

The **Pending Approval** screen appears with the request details displayed



Alberta Health Services Identity & Access Management (IAM)

Test Manager Log out Support Page

Home Self Service Access Request Reports

Pending Approval - IAM-0301231

← Return to Queue

Remote User Network Access (RUNA) - New - Pending

<p>Submitted</p> <p>04-Dec-2018 09:38:39 PM</p> <p>User: Luke Percheron</p> <p>Requester: Tester User</p> <p>Work Item Details</p>	<p>Manager Approval</p> <p>04-Dec-2018 09:38:39 PM</p> <p>Status: Waiting</p>	<p>IT Access Workitem</p> <p>Status: Not Started</p>	<p>RUNA Provision</p> <p>Status: Not Started</p>	<p>RUNA Request Completion Notification</p> <p>Status: Not Started</p>	<p>Credential Delivery</p> <p>Status: Not Started</p>
---	--	---	---	---	--

Remote User Network Access (RUNA)

RUNA Request Type: New

← Return to Queue

REVIEW the request

CLICK  [Approve](#)

The **Request Status Viewer** appears with the request showing as [Completed](#)

CLICK  [Home](#) to return to the **AHS IAM**  **Home** screen

There is one less item in your Approval Queue

In the [Request Status](#) pane the request is displayed with a status of [Completed](#)

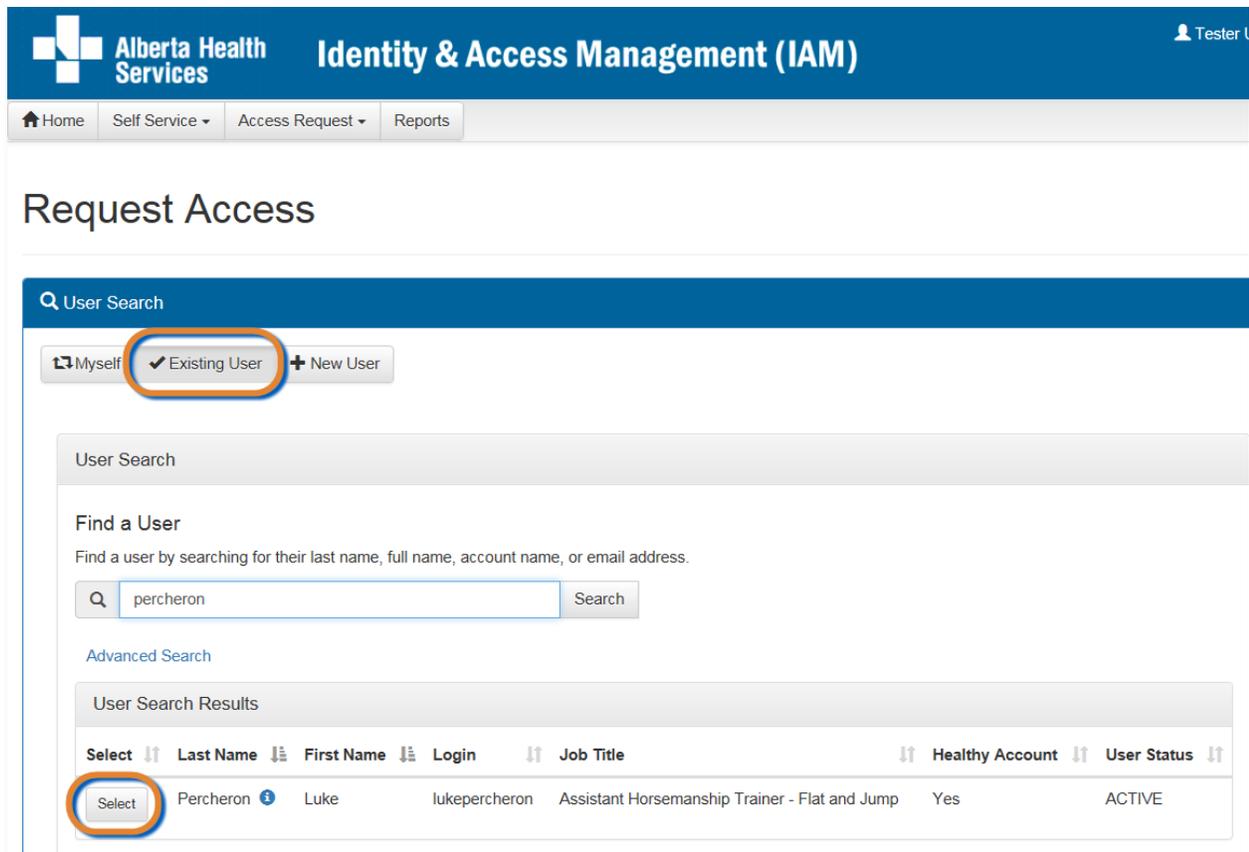
Complete 

Modify or Remove Remote Access

ENTER the AHS IAM URL into your internet web browser  <https://iam.ahs.ca>
The **AHS IAM Login** screen appears

ENTER your [Username](#) and [Password](#)
CLICK  [Log in](#)
The **AHS IAM**  **Home** screen appears

CLICK [Request or Modify Access](#)
The **Request Access** screen appears with  [Existing User](#) selected



The screenshot shows the 'Request Access' page in the AHS IAM system. At the top, there's a navigation bar with 'Home', 'Self Service', 'Access Request', and 'Reports'. The main heading is 'Request Access'. Below this, there's a 'User Search' section with three radio buttons: 'Myself', 'Existing User' (which is selected and circled in orange), and 'New User'. Underneath, there's a search box containing 'percheron' and a 'Search' button. Below the search box, there's an 'Advanced Search' link. At the bottom, there's a table titled 'User Search Results' with columns: 'Select', 'Last Name', 'First Name', 'Login', 'Job Title', 'Healthy Account', and 'User Status'. The first row of data shows 'Percheron', 'Luke', 'lukepercheron', 'Assistant Horsemanship Trainer - Flat and Jump', 'Yes', and 'ACTIVE'. The 'Select' button in the first row is circled in orange.

SEARCH for and SELECT the end-user
The **Request Access** screen appears with the end-user's details displayed

At [Available Entitlements](#), under [Remote User Network Access \(RUNA\)](#), CLICK [Change Access](#)
The screen refreshes
The [Selected Entitlements](#) pane appears at the bottom of the screen with [Remote User Network Access \(RUNA\)](#) displayed


Identity & Access Management (IAM)

[Home](#) | [Self Service](#) | [Access Request](#) | [Reports](#)

Request Access

Selected User For Request

Name: Luke Percheron
User Name: lukepercheron
IGUID: TTTTIIY
Account Type: Non-Employee
Email:
Phone: 587-555-8877
Status: ACTIVE

[Select a Different User](#)

Available Entitlements

Alberta Netcare Portal <small>Used to request a Netcare and PIN/PD account. NOTE: This will also request a new Base Health System account needed to manage your identity profile and password.</small>	Request Access
CPAR User Registration (CPAR) <small>Request/remove access for Central Patient Attachment Registry (CPAR).</small>	Request Access
Network Account (NAR) <small>Request the creation, amendment, reactivation, rename, termination of an AHS non-employee account or request an emergency termination of an AHS employee.</small>	Change Access
PrescribeIT <small>Request/remove access for PrescribeIT account (PxIT).</small>	Request Access
Shared Drive/Folder (Existing) <small>Request/remove access to an existing network shared drive or existing shared drive folder.</small>	Request Access
Shared Drive/Folder (New) <small>Request the creation of a new network shared drive or a new restricted folder on an existing shared drive on the AHS network.</small>	Request Access

Selected Entitlements

Remote User Network Access (RUNA) <small>Request the ability to remotely access the AHS network.</small>	Remove from Request
--	-------------------------------------

Next
Cancel

CLICK **Next**

The **Complete Access Request** screen appears with the end-user's details displayed.

MODIFY the  **Remote User Network Access (RUNA)** pane as needed

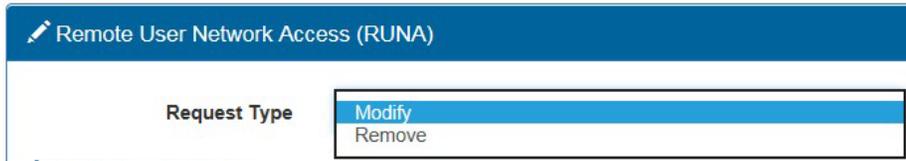
READ the on-screen information and field tips

SEE the  **Tool Tips** on the following page

Tool Tips for the Complete Access Request Screen

At Request Type

SELECT **Modify** or **Remove** from the dropdown list



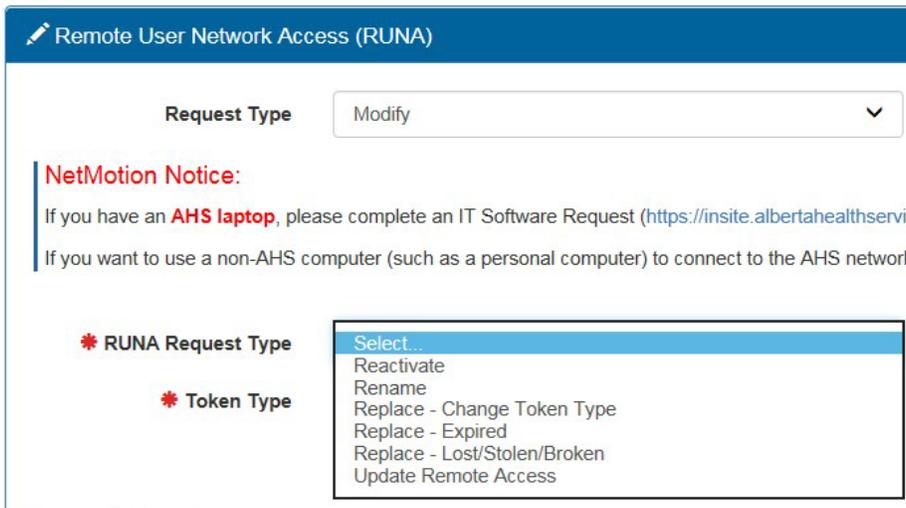
Remote User Network Access (RUNA)

Request Type: Modify
Remove

Modify	Change the end-user's remote access criteria on their already approved AHS IAM identity account.
Remove	Remove the end-user's remote access from their AHS IAM identity account.

At RUNA Request Type

SELECT the most appropriate value form the dropdown list



Remote User Network Access (RUNA)

Request Type: Modify

NetMotion Notice:
If you have an **AHS laptop**, please complete an IT Software Request (<https://insite.albertahealthservices.ca/itsoftware>)
If you want to use a non-AHS computer (such as a personal computer) to connect to the AHS network, please contact the IT Helpdesk.

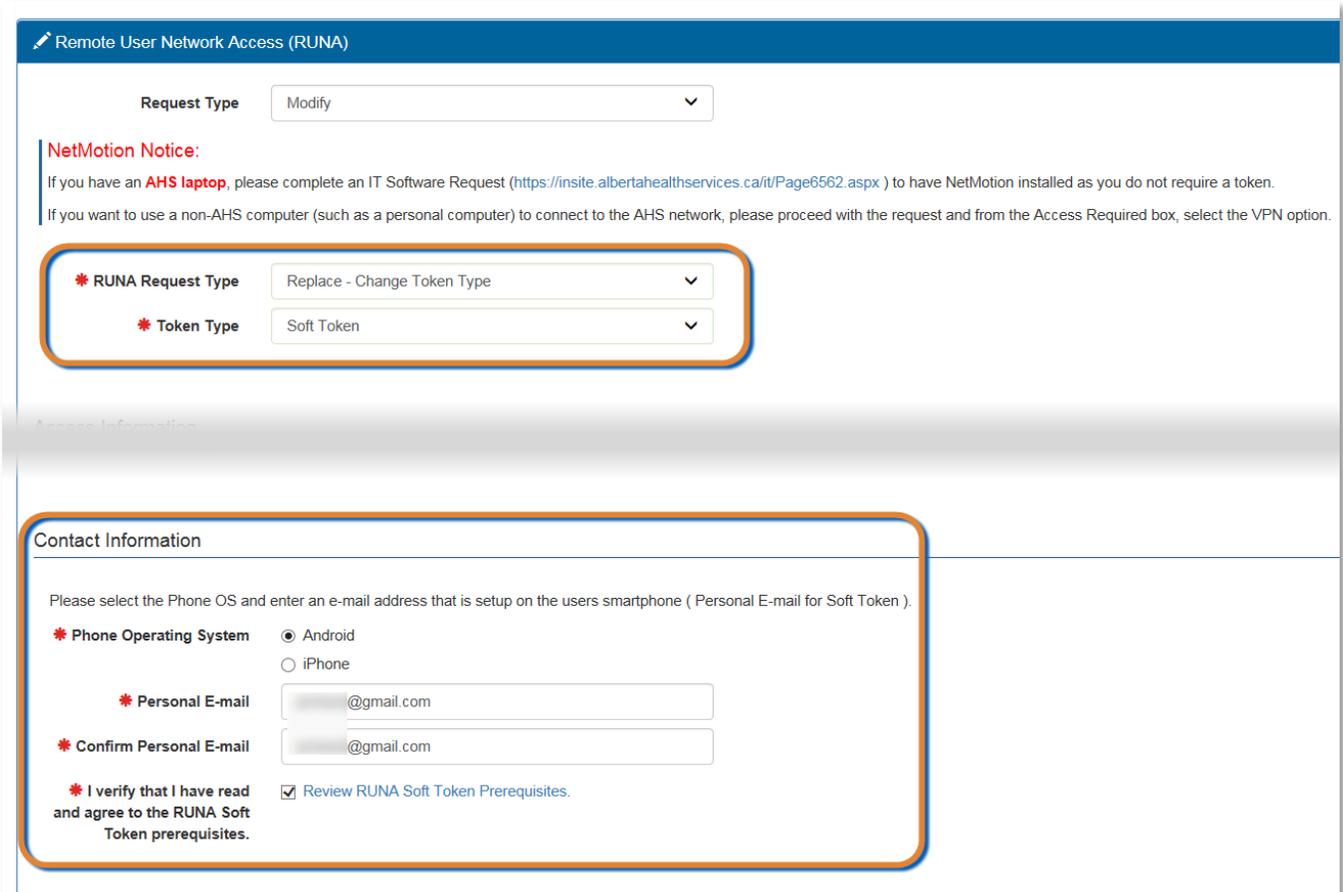
* RUNA Request Type
* Token Type

Select...
Reactivate
Rename
Replace - Change Token Type
Replace - Expired
Replace - Lost/Stolen/Broken
Update Remote Access

Reactivate	Enable a remote access account that was disabled or removed due to inactivity or termination
Rename	Change end-user's name
Replace – Change Token Type	Change a hard SecurID token to a software token or vice versa
Replace – Expired	Initiate sending out a replacement token
Replace – Lost/Stolen/Broken	Initiate sending out a replacement token
Update Remote Access	Change the access required. E.g. end-user has VPN access but also needs MyApps / UAP access

In the sample below, we chose “[Replace – Change Token Type](#)”; we are requesting a change from a hard to a soft token. This required us to enter an external email address and a smart phone operating type.

Many of the [Request Types](#) require you to enter corresponding information – check the screen carefully before submitting the request.



Remote User Network Access (RUNA)

Request Type:

NetMotion Notice:
 If you have an **AHS laptop**, please complete an IT Software Request (<https://insite.albertahealthservices.ca/it/Page6562.aspx>) to have NetMotion installed as you do not require a token.
 If you want to use a non-AHS computer (such as a personal computer) to connect to the AHS network, please proceed with the request and from the Access Required box, select the VPN option.

* RUNA Request Type:

* Token Type:

Contact Information

Please select the Phone OS and enter an e-mail address that is setup on the users smartphone (Personal E-mail for Soft Token).

* Phone Operating System: Android iPhone

* Personal E-mail:

* Confirm Personal E-mail:

* I verify that I have read and agree to the RUNA Soft Token prerequisites. [Review RUNA Soft Token Prerequisites.](#)

CLICK [Submit](#)

The **Request Status Viewer** appears with the request displayed as [Waiting for Manager Approval](#).

If you are an [Authorized Approver](#), you will not have to select an [Authorized Approver](#). The request will be automatically approved when you submit the request.

CLICK  [Home](#) to return to the **AHS IAM**  **Home** screen

In the [Request Status](#) pane, the request appears with a Status of [Pending](#)

The request requires approval by the [Authorized Approver](#)

Complete 

Setting up your RSA SecurID Token

NOTE:

These processes must be performed by the end-user of the RSA SecurID token.

NOTE:

You will be sent a number of emails from Identity Management and IT Access Remote Access. The Identity Management emails confirm the RUNA request has been submitted / completed. The IT Access Remote Access emails provide important security information and installation instructions. We are providing the installation instructions here – but you must use the emails sent to you because they include unique links.

SUPPORTS:

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.

Hard Token Set Up

If you requested a Hard Token it will be mailed to you together with PIN set up instructions.

Soft Token Set Up

Look for email from IT Access Remote Access with a subject line that says, “Your RSA SecurID Software Token – IAM Request#...”.

The hyperlinks and QR codes in that email are unique to you and are good for 30 days from the date the mail was sent to you. If you haven’t set up your token within that time, contact the AHS IT Service Desk 1 877 311 4300 to request fresh instructions.

If the email did not arrive on the device you want your soft token on, forward it to the email address associated with that device. Keep the original email as the hyperlinks and attachments may not open properly on all devices.

If you want your soft token on a tablet or computer, these instructions should work for those devices. If you run into problems, please contact the AHS IT Service Desk 1 877 311 4300 for help from them or from the IT Access Remote Access team.

Follow these four steps on either an Apple or Android device.

Step 1 of 4: Install the RSA SecurID App on your Device – Apple or Android

Step 2 of 4: Import your unique token into the app

Step 3 of 4: Set up your Personal Identification Number (PIN)

Step 4 of 4: Use your soft token

Step 1 of 4: Install the RSA SecurID App on your Device – Apple or Android

If you already have the app installed, move onto Step 2.



[Apple App Store Link](#)

INSTALL the app on your iPhone or other device

[Google \[Android\] Play Store Link](#)

INSTALL the app on your smartphone or other device

Step 2 of 4: import your unique token into the app

CHOOSE one of these 3 methods to link your unique token to the app on your device.

Method 1 – Clicking the link from your Smartphone

Method 2 – SDTID File

Method 3 – QR Code

Method 1 – Clicking the Link From Your Smartphone

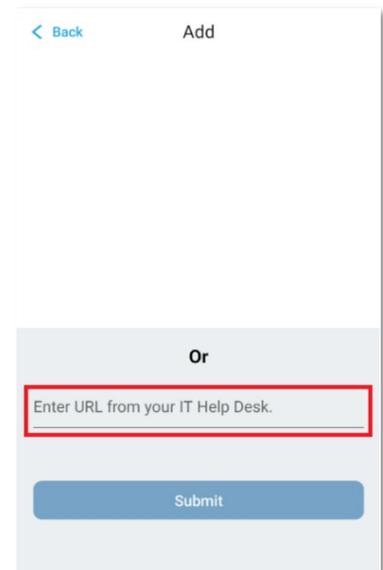
Your email from IT Access Remote Access will include unique links for you to use.

CLICK on either the Android link or the Apple link

The link should open the RSA app on your device, importing your unique information automatically.

iPhone Note: Some email clients will not recognize the link provided to you. Try using the built-in mail app. If you are using an AHS email, the built-in mail app will not work.

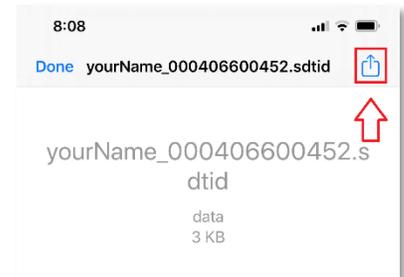
iPhone and Android Note: If clicking the link does not work, you can try to copy / paste the link into the into the box in the RSA SecurID app. See screen shot.



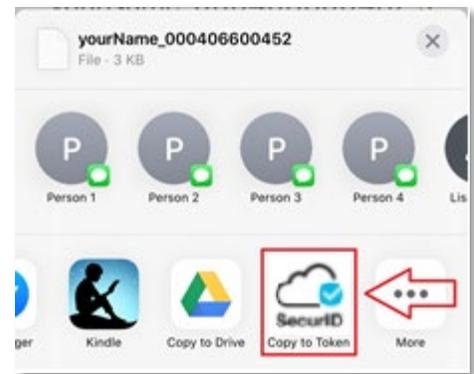
Method 2 – SdTID File

OPEN the email from IT Access Remote Access on your device
CLICK on the SdTID file attached to the email

iPhone Note: SELECT the share icon.



You may need to swipe left to find the RSA Token App.



SELECT RSA Token App

You should see a “Token imported successfully” message

Method 3 – QR Code

USE a different device than the one you want your soft token on

OPEN the “Your RSA SecurID Software Token...” email from the IT Access Remote Access

OPEN the SecurID Authenticator app and click "Get Started" OR CLICK the plus + symbol in the top right corner

SCAN the QR code for your device and it should import your token

Your email will have Apple and Android QR codes that are unique to you

Setting your PIN

NOTE:

You must set up a 4-digit Personal Identification Number (PIN) that protects your token. It is the unique combination of your token's serial number, your PIN, and the generated passcode that authenticates you to the system you're trying to log into. Your PIN is stored on AHS servers and will not change unless you change it. Your PIN can be used with the SecurID app on a new phone, a difference device, even if you delete the app and install it again.

NOTE:

Hard token: You will enter your PIN plus the 6-digits that appear on your hard token to authenticate your remote access.

NOTE:

Soft token: You will enter your PIN into the RSA SecurID app to generate a passcode. Then you will enter ONLY the 8-digit generated passcode to authenticate your remote access. Fun fact: you can enter any four numbers into the app to generate a passcode. But that passcode won't work for you.

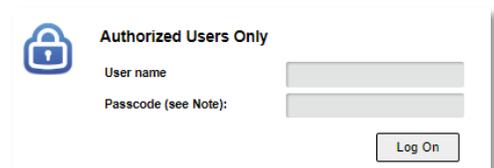
You may need two devices for this process. If the device you want your token on is an AHS device, you will need a non-AHS device to help you complete the set up. If the device you want your token is not an AHS device, you will only need that device to complete the set up.

On the device you want your token on

LAUNCH the RSA SecurID App
In the PIN field, ENTER 0000

On the non-AHS device

GO TO token.albertahealthservices.ca
CLICK "Proceed" or "Accept" to any certificate or security notices
ENTER your unique username provided in the IT Access Remote Access email
ENTER only the 8-digit passcode displayed in the app
You will be prompted to create your PIN



ENTER 4 to 8 alphanumeric characters – do not begin with a zero “0”

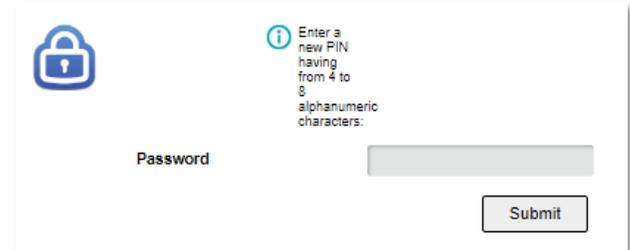
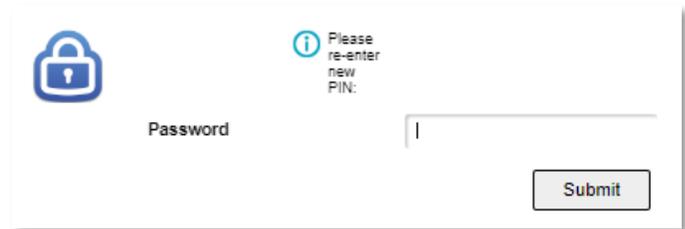
MEMORIZE your PIN

CLICK Submit

You will be prompted to re-enter your PIN

RE-ENTER your PIN

CLICK Submit

On the device you want your token on

CLOSE the SecurID app

REOPEN the SecurID app

You will be prompted for a PIN

ENTER your PIN

A passcode will appear on the app

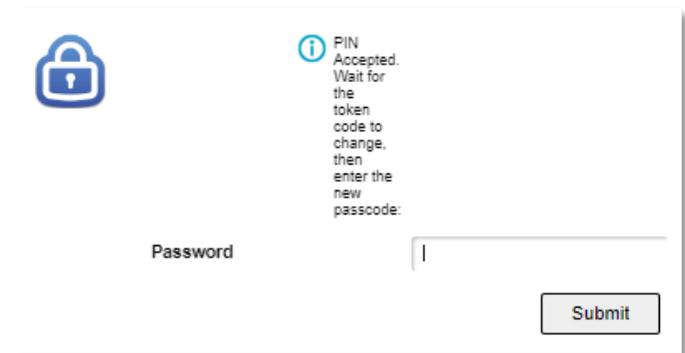
WAIT for the next passcode to appear and ...

On the non-AHS device

ENTER the second passcode (8-digits) that appears on your SecurID app

This step can occasionally prompt an error. Please verify that your soft token works by logging into an application remotely. E.g., [Log into AHS IAM Remotely](#), further in this guide.

If you have issues contact the [Supports](#) listed earlier in this section.



Incorrect login attempts

If your login is unsuccessful, wait for the token code to change and try again.

After three (3) incorrect login attempts you will be locked out of your remote access account for 15 minutes. You can try again after that time.

Inactive access

All remote access accounts are monitored for inactivity. Inactive accounts are a security vulnerability. If you have not used your remote access in 180 days (approximately 6 months) your token will be deactivated and you'll have to request a new one.

Tokens expire

Hard and soft tokens don't last forever. Discover your token's expiry date and request a replacement token before that time. Please see the [Remote Access with RSA SecurID Tokens Fact Sheet](#) for complete instructions.

Have you forgotten your PIN?

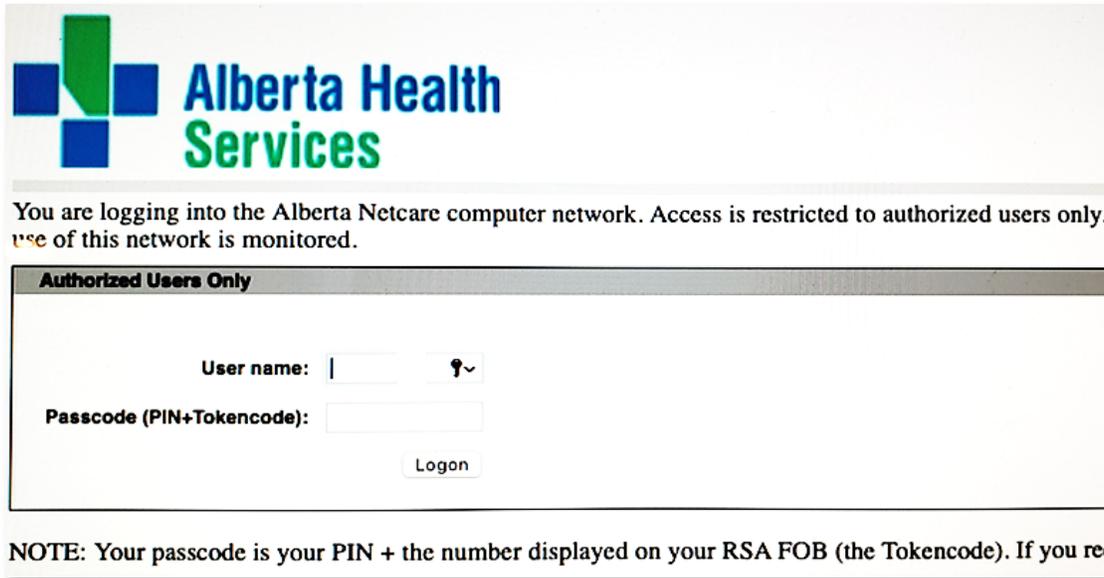
Contact the [Supports](#) listed earlier in this guide.

Complete 

Log into AHS IAM Remotely

Use this login as an example of how to log into an AHS application remotely.

ENTER the AHS IAM URL into your internet web browser  <https://iam.ahs.ca>
The **AHS Citrix Gateway** login screen appears



The screenshot shows the AHS IAM login interface. At the top left is the Alberta Health Services logo. Below it, a warning message reads: "You are logging into the Alberta Netcare computer network. Access is restricted to authorized users only. Use of this network is monitored." Below the warning is a section titled "Authorized Users Only" which contains a "User name:" field with a dropdown arrow, a "Passcode (PIN+Tokencode):" field, and a "Logon" button. At the bottom of the screenshot, a note states: "NOTE: Your passcode is your PIN + the number displayed on your RSA FOB (the Tokencode). If you receive..."

ENTER your [Username](#)



Tool Tip – this is your AHS Network UserID or your AHS IAM Username

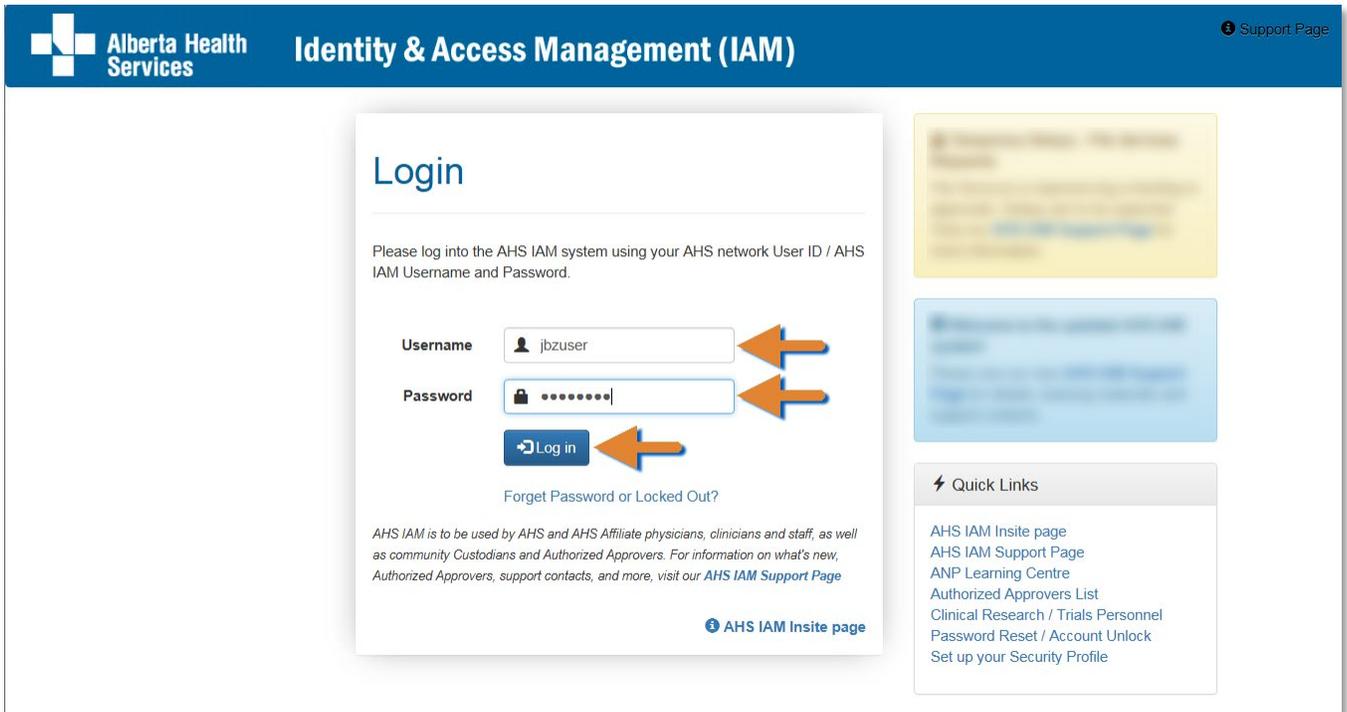
ENTER your [Passcode](#)

If a hard [SecurID token](#), enter your 4-digit PIN followed by the 6 numbers displayed on the SecurID token into the [Passcode](#) field – 10 digits in total.

If a soft [SecurID token](#), enter your PIN and SUBMIT to generate a code. Enter the 8 numbers displayed in the app window into the [Passcode](#) field – 8 digits in total.

CLICK [Logon](#)

The **AHS IAM Login** screen appears



ENTER your Username and Password

CLICK  Log in

The AHS IAM  Home screen appears

Complete 

Appendix – AHS IAM Terms & Definitions

These may or may not be the same as your organization’s definitions.

AHS Employee	A person on-boarded and paid through AHS Human Resources e-People
AHS Non-Employee	A person not on-boarded or paid through AHS Human Resources e-People
Community End-User	A person who works for a privately owned health delivery facility. Examples: physician, pharmacist, dentist, chiropractor.
Combination End-User	A person who is more than one of the above types.
Requester	A person who submits a RUNA request in AHS IAM. If the requester is an Authorized Approver , the request will be automatically approved. If the requester is not an Authorized Approver , they will have to identify one in the request.
Authorized Approver	<p>A person who is able to approve access requests in AHS IAM. An Authorized Approver must meet one of these criteria.</p> <ul style="list-style-type: none"> Have an AHS Delegation of Human Resources Authority (DOHRA) of 1 to 12 OR Have a Covenant Health DOHRA of 1 to 6, 9 to 12 OR Be pre-approved by AHS IT Access to perform the role of an Authorized Approver. Only available when a DOHRA structure is not. <p>More information about Authorized Approvers can be found on the AHS IAM Support Page, under  Authorized Approvers.</p> <p>Click here to view the AHS IAM list of Authorized Approvers for AHS Affiliates only – NAR, RUNA, ANP and I/Request only.</p>

◆ end ◆