EXECUTIVE SUMMARY

UTLogin provides centralized authentication (single sign-on) services for more than 250 campus systems through a combination of Web Policy Agents (WPAs) installed on on-campus servers as well as SAML federation with off-campus systems. UTLogin processes more than 55 million authentication requests annually.

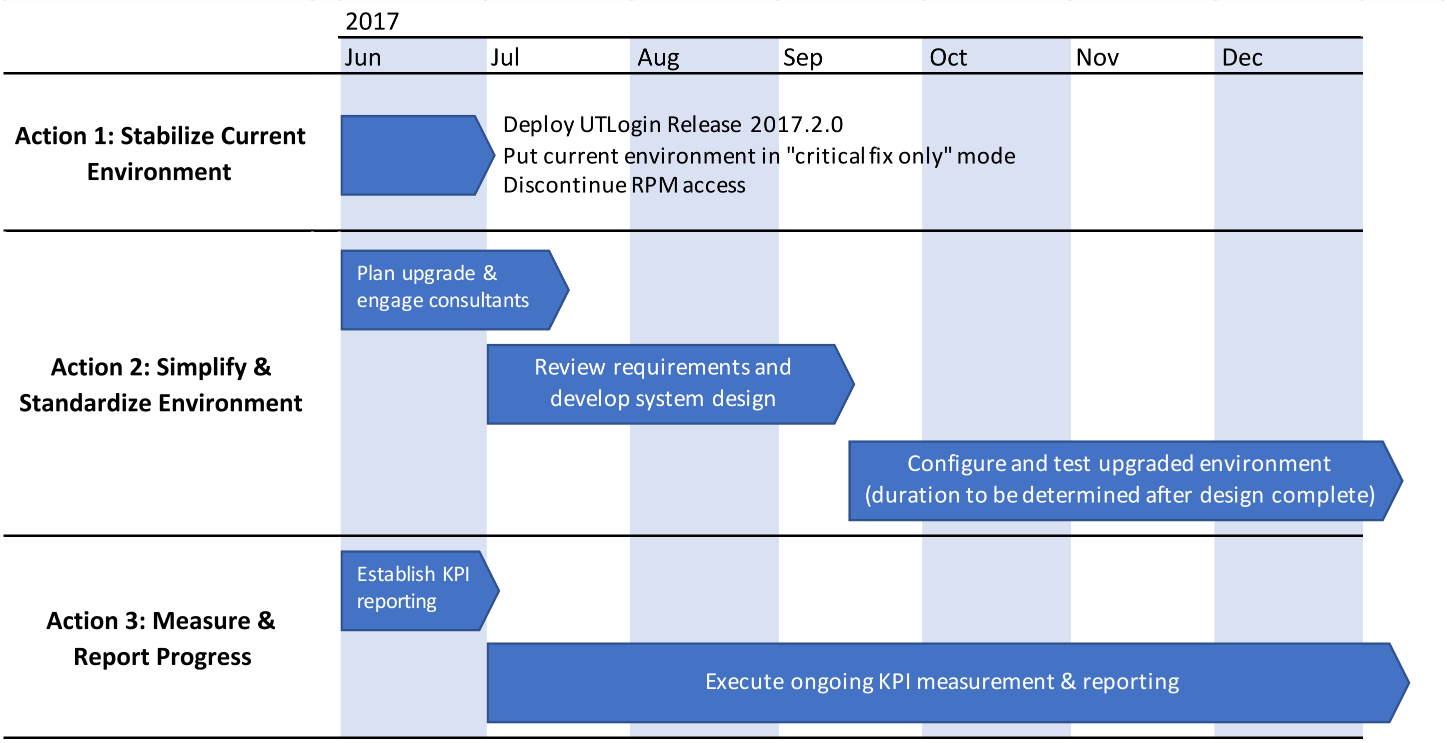
A marked increase in UTLogin service interruptions and system instability began in the summer of 2016. Although mitigations and fixes have been implemented to address each issue, new issues with different causes continue to appear. The Identity and Access Management (IAM) team believes the overall root cause of the ongoing instability is a combination of three major factors:

- Maintenance complexity and support issues related to customizations and non-standard configuration of the base OpenAM vendor product implemented within UTLogin
- Aging UTLogin system components that are at or near end of life
- An increase in the number and complexity of the sites being protected by UTLogin

The IAM team is taking the following actions to return UTLogin to reliable and stable operation:

- **Action 1: Stabilize Current UTLogin Environment** – Keep the current environment as stable as possible by putting the system in a "critical fix only" mode and limiting unproductive investment of time in the current environment.
- **Action 2: Simplify & Standardize UTLogin Environment** – Upgrade system components to current supported versions, remove customizations and non-standard configurations of the base OpenAM product, minimize external dependencies, and review and simplify the authentication policy model.
- **Action 3: Measure & Report Progress** – Monitor key performance indicators (KPIs) and report progress toward improving stability to UTLogin stakeholders.

Work on all three actions is either already in progress or will start in June 2017:



CURRENT SITUATION SUMMARY AND ISSUES SINCE SUMMER 2016

Since the summer of 2016, UTLogin has experienced a significant number of service disruptions (see Appendix). Of the 20 UTLogin service incidents that have occurred between June 2016 and May 2017, 8 were caused by customizations or non-standard configurations. 3 additional incidents were caused by human error, some of which were exacerbated by customizations within UTLogin. The remaining incidents were caused by issues in external dependencies (such as DNS or load balancing services), vendor code bugs, or a mix of causes. Figure 1 below summarizes the incidents by cause.

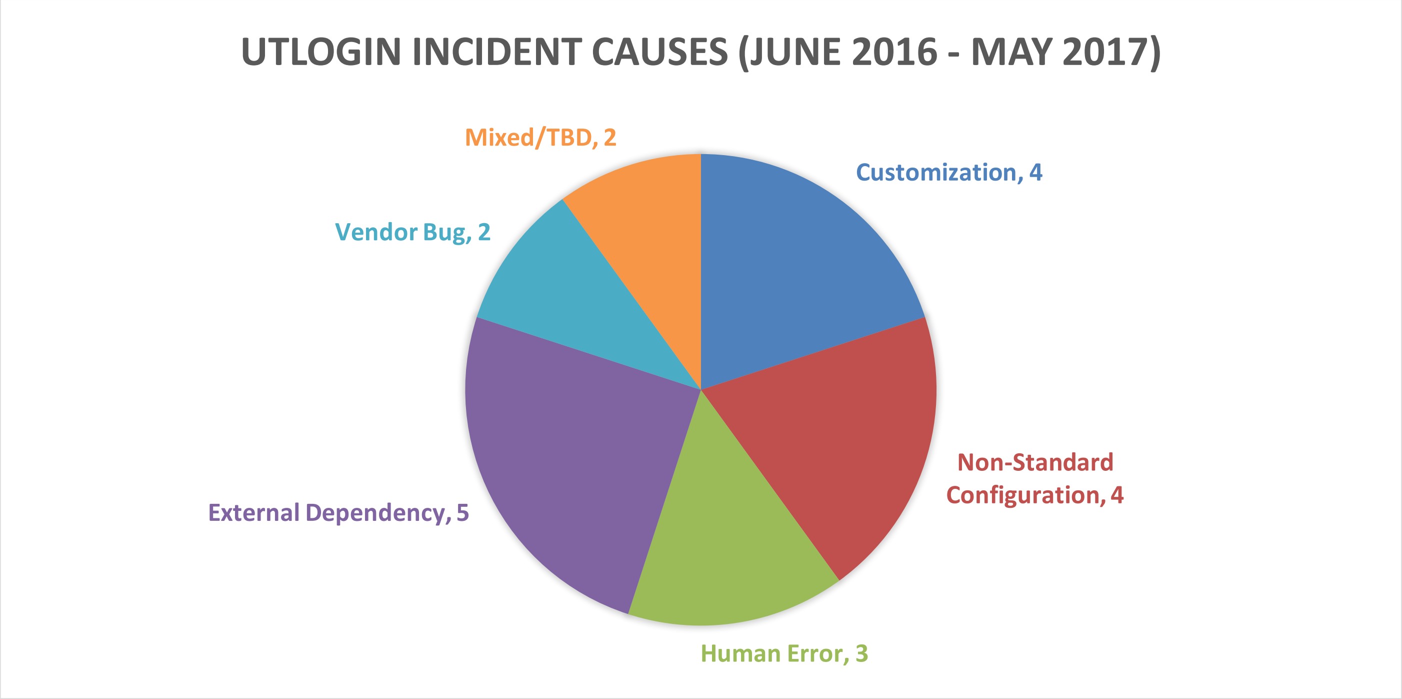


Figure 1: UTLogin Incident Causes

For each service disruption, the IAM team has completed a root cause analysis and implemented fixes and mitigations. However, additional incidents continue to occur on a regular basis, indicating a broader problem. The IAM team believes that there are three major factors contributing to the overall stability problem:

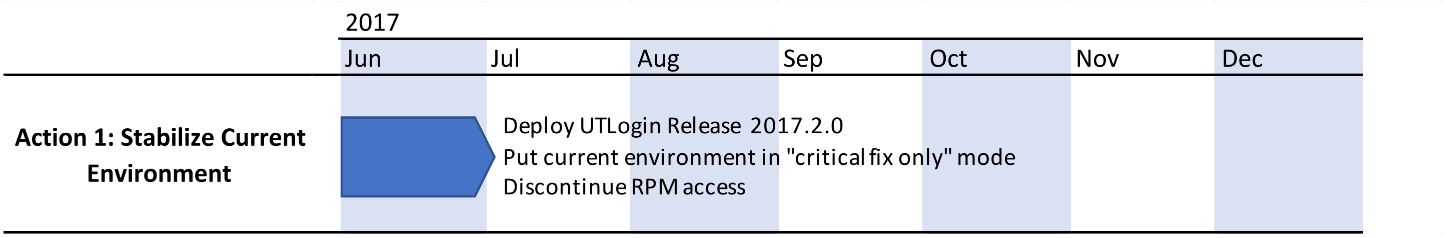
- **Customizations and non-standard configuration** – UTLogin relies on the OpenAM vendor product to provide authentication services. OpenAM was heavily customized and configured in non-standard ways during the original implementation of UTLogin to meet unique UT Austin requirements. These customizations and non-standard configurations have directly caused some outages and have made diagnosis and resolution of other outages more difficult. Staff turnover has resulted in a loss of technical understanding of the customizations, making it challenging to maintain them properly.
- **Aging system components** – The UTLogin system components have been in Production use since 2013 and are at or approaching end of life. Support from both vendors and ITS Systems to maintain these components will not be available in the near future. Investing more time and resources in patching problems in the current aging system infrastructure is not productive.
- **Changing demands on the UTLogin system** – Since UTLogin was implemented the number and complexity of sites participating in the UTLogin environment have greatly increased. In particular, the implementation of UT Web introduced a large and complex new set of demands on the system. The existing customizations to the OpenAM product were further customized to try to address these new demands, inadvertently making the system more fragile and difficult to maintain.

ROADMAP FOR OPERATIONAL STABILITY

To address the UTLogin service issues, the IAM team will **stabilize and limit changes** to the current system environment, **simplify and standardize** the service while upgrading its components, and **measure and report progress** toward operational stability.

ACTION 1: STABILIZE AND LIMIT CHANGES TO CURRENT UTLOGIN ENVIRONMENT

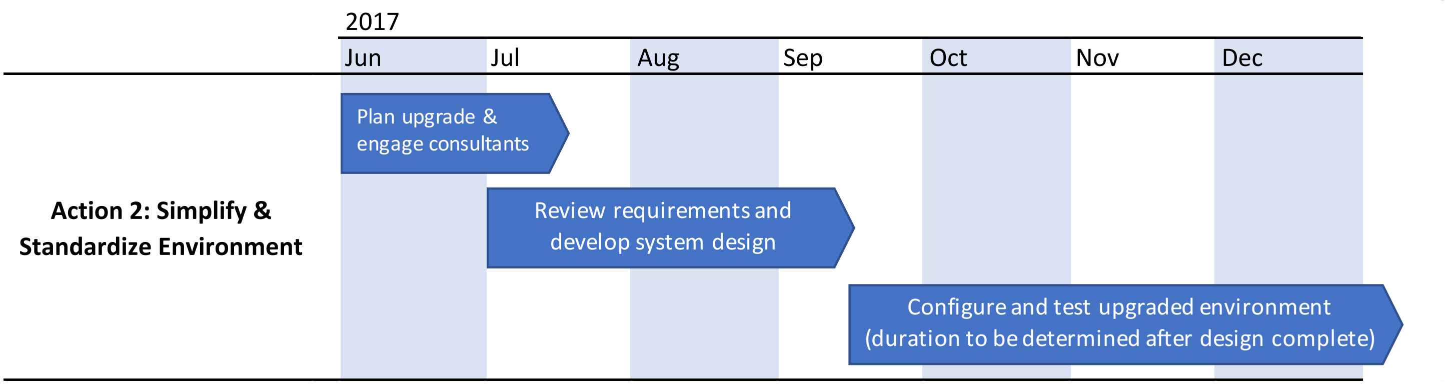
Effective with the deployment of UTLogin Release 2017.2.0 on June 4, 2017, the current UTLogin system environment will be operated in a “critical fix only” mode and all configuration changes will be strictly limited. Modifications to the current environment will only be made to address critical Production outages or security issues. Enhancements to UTLogin functionality will be deferred until Action 2 (described below) is complete. College, School, and Unit (CSU) access to the custom Realm Policy Manager (RPM) will be suspended. Changes to CSU authentication policies will be made by the IAM team upon request in a regularly scheduled maintenance process.



ACTION 2: SIMPLIFY AND STANDARDIZE UTLOGIN ENVIRONMENT

The IAM team will focus on simplifying and standardizing the UTLogin environment. UTLogin system components will be upgraded to current and well-supported versions. During this upgrade, customizations and non-standard configurations of OpenAM will be removed. Specifically, native capabilities will be used for whitelist filtering and brute force attack defenses. UTLogin’s current dependency on TED will also be removed. Reliance on external dependencies like DNS and load balancing services will be reduced to the bare minimum. The authentication policy model will be simplified while preserving the ability for CSUs to maintain their own policies, if possible.

Expert OpenAM consultants will be engaged to review UTLogin requirements and the design for the updated UTLogin environment. They will also provide cost and schedule proposals for deploying the new environment, with options for accelerating development, testing, and implementation of the new environment.

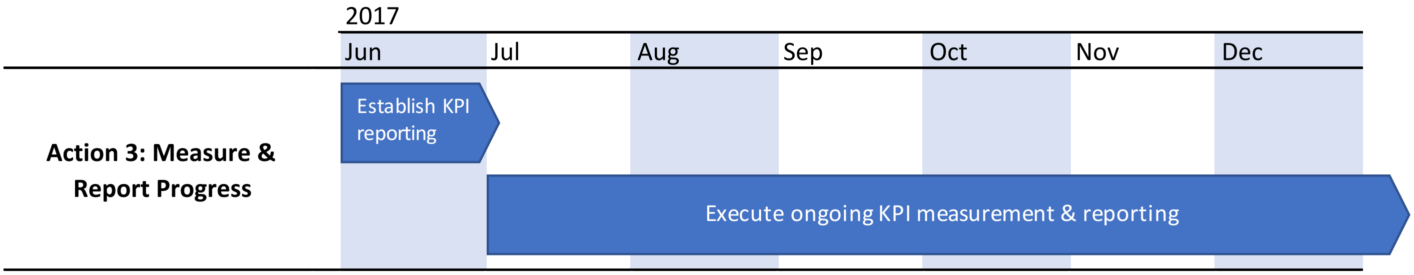


ACTION 3: MEASURE AND REPORT PROGRESS

Key Performance Indicators (KPIs) will be established for the UTLogin service. These KPIs will measure whether UTLogin is meeting the core needs of its users to be able to authenticate to campus systems integrated with UTLogin:

- When a login page is requested, does UTLogin provide one?
- When a user attempts to log in, does UTLogin successfully validate the user’s credentials?
- When a user authenticates successfully, does UTLogin return an accurate access policy decision to the system being accessed by the user?

A web site will be established to display KPIs in a graphical format and will be updated on a weekly basis. Stakeholders will receive a monthly service summary, including KPI information, via email.



APPENDIX: UTLOGIN SERVICE INCIDENTS JUNE 2016 TO MAY 2017

The table below lists UTLogin service incidents from June 2016 to May 2017:

Date	Incident Description	Outage Minutes	Cause Type
06/13/2016	TED issue causes UTLogin outage	55 (partial)	Non-Standard Configuration
07/27/2016	Bug in UTLogin custom code causes degradation	0	Customization
08/11/2016	TED issue causes UTLogin outage	285 (partial)	Non-Standard Configuration
08/24/2016	Bug in OpenAM code causes UTLogin outage	3 (partial)	Vendor Issue
09/12/2016	Bug in OpenAM code causes UTLogin outage	19 (partial)	Vendor Issue
09/28/2016	DNS issue causes UTLogin outage	21 (partial)	External Dependency
10/05/2016	F5 issue causes UTLogin outage	15 (total)	External Dependency
10/13/2016	F5 issue causes UTLogin outage	11 (total)	External Dependency
11/21/2016	Unexpected behavior in custom code causes outage	9 (partial)	Customization
12/06/2016	TED issue causes UTLogin outage	60 (partial)	Non-Standard Configuration
12/12/2016	TED issue causes UTLogin outage	4 (total)	Non-Standard Configuration
01/08/2017	Unexpected configuration behavior causes outage	137 (total)	Mixed
01/13/2017	Bug in UTLogin custom code causes 2FA outage	780 (partial)	Customization
02/21/2017	Misconfiguration in UTLogin 2FA – No Prod impact	0	Human error
04/06/2017	Unexpected behavior in custom code causes outage	2 (total)	Customization
04/08/2017	SSL certificate expiration causes outage	120 (total)	Human error
05/10/2017	Authentication policy errors cause outage	93 (partial)	*Under investigation*
05/17/2017	DNS issue causes UTLogin outage	55 (partial)	External Dependency
05/18/2017	Misconfiguration causes UTLogin outage	15 (partial)	Human error
05/23/2017	DNS issue causes UTLogin outage	54 (partial)	External Dependency